EUROPEAN PARLIAMENT

1999 *2004*

Session document

FINAL
A5-0264/2001
PAR1

11 July 2001

REPORT

on the existence of a global system for the interception of private and commercial communications (ECHELON interception system) (2001/2098(INI))

Part 1: Motion for a resolution
Explanatory statement

Temporary Committee on the ECHELON Interception System

Rapporteur: Gerhard Schmid

'Sed quis custodiet ipsos custodes.'
Juvenal (ca. 60 to 130 AD), Sat. 6, 347

CONTENTS

Page

PROCEDURAL PAGE 9

MOTION FOR A RESOLUTION 10

EXPLANATORY STATEMENT 21

1. **Introduction: 21**

1.1. The reasons for setting up the committee 21
1.2. The claims made in the two STOA studies on a global interception system codenamed ECHELON 21
1.2.1. The first STOA report of 1997 21
1.2.2. The 1999 STOA reports.....21
1.3. The mandate of the committee 22
1.4. Why not a committee of inquiry? 22
1.5. Working method and schedule 23
1.6. Characteristics ascribed to the ECHELON system 23

2. The operations of foreign intelligence services…….....25

2.1. Introduction 25
2.2. What is espionage? 25
2.3. Espionage targets 25
2.4. Espionage methods 25
2.4.1. Human intelligence.....26
2.4.2. Processing of electromagnetic signals 26
2.5. The operations of certain intelligence services.....27

3. Technical conditions governing the interception of telecommunications.....30

3.1. The interceptibility of various communication media.....30
3.2. The scope for interception on the spot 30
3.3. The scope for a worldwide interception system 31
3.3.1. Access to communication media 31
3.3.2. Scope for the automatic analysis of intercepted communications: the use of filters 35
3.3.3. The example of the German Federal Intelligence Service.....35

4. Satellite communications technology 37

4.1. The significance of telecommunications satellites 37
4.2. How a satellite link operates 38
4.2.1. Geostationary satellites 38
4.2.2. The route followed by signals sent via a satellite communication link 38
4.2.3. The most important satellite communication systems 39
4.2.4. The allocation of frequencies 43
4.2.5. Satellite footprints 43
4.2.6. The size of antennae required by an earth station 44
4.3. Satellite communications for military purposes 45
4.3.1. General 45
4.3.2. Frequencies used for military purposes 45
4.3.3. Size of the receiving stations 45
4.3.4. Examples of military communications satellites 45

5. Clues to the existence of at least one global interception system 47

5.1. Why is it necessary to work on the basis of clues? 47
5.1.1. Evidence of interception activity on the part of foreign intelligence services 47
5.1.2. Evidence for the existence of stations in the necessary geographical areas 47
5.1.3. Evidence of a close intelligence association 48
5.2. How can a satellite communications interception station be recognised? 48
5.2.1. Criterion 1: accessibility of the installation 48
5.2.2. Criterion 2: type of antenna 48
5.2.3. Criterion 3: size of antenna 49
5.2.4. Criterion 4: evidence from official sources 49
5.3. Publicly accessible data about known interception stations 50
5.3.1. Method 50
5.3.2. Detailed analysis 50
5.3.3. Summary of the findings 59
5.4. The UKUSA Agreement 59
5.4.1. The historical development of the UKUSA Agreement 59
5.4.2. Evidence for the existence of the agreement 61
5.5. Evaluation of declassified American documents 62
5.5.1. Nature of documents 62
5.5.2. Content of documents 63
5.5.3. Summary 66
5.6. Information from authors and journalists specialised in this field 67
5.6.1. Nicky Hager's book 67
5.6.2. Duncan Campbell 68
5.6.3. Jeff Richelson 69
5.6.4. James Bamford 69
5.6.5. Bo Elkjaer and Kenan Seeberg 70
5.7. Statements by former intelligence service employees 71
5.7.1. Margaret Newsham (former NSA employee) 71
5.7.2. Wayne Madsen (former NSA employee) 71
5.7.3. Mike Frost (former Canadian secret service employee) 71

5.7.4. Fred Stock (former Canadian secret service employee) 72
5.8. Information from government sources 72
5.8.1. USA 72
5.8.2. UK 72
5.8.3. Australia 73
5.8.4. New Zealand 73
5.8.5. The Netherlands 73
5.8.6. Italy 74
5.9. Questions to the Council and Commission 74
5.10. Parliamentary reports 75
5.10.1. Reports by the Comité Permanent R, Belgium's monitoring committee 75
5.10.2. Report by the French National Assembly's Committee on National Defence 75
5.10.3. Report of the Italian Parliament's Committee on Intelligence and Security Services and State Security 76

6. Might there be other global interception systems? 77

6.1. Requirements of such a system 77
6.1.1. Technical and geographical requirements 77
6.1.2. Political and economic requirements 77
6.2. France 77
6.3. Russia 78
6.4. The other G-8 States and China 79

7. Compatibility of an 'ECHELON' type communications interception system with Union law 80

7.1. Preliminary considerations 80
7.2. Compatibility of an intelligence system with Union law 80
7.2.1. Compatibility with EC law 80
7.2.2. Compatibility with other EU law 81
7.3. The question of compatibility in the event of misuse of the system for industrial espionage 82
7.4. Conclusion 82

8. The compatibility of communications surveillance by intelligence services with the fundamental right to privacy 83

8.1. Communications surveillance as a violation of the fundamental right to privacy 83
8.2. The protection of privacy under international agreements 83
8.3. The rules laid down in the ECHR 84
8.3.1. The importance of the ECHR in the EU 84
8.3.2. The geographical and personal scope of the protection provided under the ECHR 85
8.3.3. The admissibility of telecommunications surveillance pursuant to Article 8 of the ECHR 85
8.3.4. The significance of Article 8 of the ECHR for the activities of intelligence services) 86

8.4. The requirement to monitor closely the activities of other countries' intelligence services 87
8.4.1. Inadmissibility of moves to circumvent Article 8 of the ECHR through the use of other countries' intelligence services 87
8.4.2. Implications of allowing non-European intelligence services to carry out operations on the territory of Member States which are ECHR contracting parties 88

9. Are EU citizens adequately protected against the activities of intelligence services? 91

9.1. Protection against the activities of intelligence services: a task for the national parliaments 91
9.2. The powers enjoyed by national authorities to carry out surveillance measures 91
9.3. Monitoring of intelligence services 92
9.4. Assessment of the situation for European citizens 95

10. Protection against industrial espionage 97

10.1. Firms as espionage targets 97
10.1.1. Espionage targets in detail 97
10.1.2. Competitive intelligence 98
10.2. Damage caused by industrial espionage 98
10.3. Who carries out espionage? 99
10.3.1. Company employees (insider crime) 99
10.3.2. Private espionage firms 100
10.3.3. Hackers 100
10.3.4. Intelligence services 100
10.4. How is espionage carried out? 100
10.5. Industrial espionage by states 101
10.5.1. Strategic industrial espionage by the intelligence services 101
10.5.2. Intelligence services as agents of competitive intelligence 101
10.6. Is ECHELON suitable for industrial espionage? 102
10.7. Published cases 102
10.8. Protection against industrial espionage 107
10.8.1. Legal protection 107
10.8.2. Other obstacles to industrial espionage 107
10.9. The USA and industrial espionage 108
10.9.1. The challenge for the US Administration: industrial espionage against US firms 109
10.9.2. The attitude of the US Administration towards active industrial espionage 110
10.9.3. Legal situation with regard to the payment of bribes to public officials 111
10.9.4. The role of the Advocacy Center in promoting US exports 112
10.10. Security of computer networks 114
10.10.1. The importance of this chapter 114
10.10.2. The risks inherent in the use by firms of modern information technology 114
10.10.3. Frequency of attacks on networks 116
10.10.4. Perpetrators and methods 116
10.10.5. Attacks from outside by hackers 117

10.11. Under-estimation of the risks....117
10.11.1. Risk-awareness in firms....117
10.11.2. Risk-awareness among scientists....118
10.11.3. Risk-awareness in the European institutions....118

11. Cryptography as a means of self-protection....120

11.1. Purpose and method of encryption....120
11.1.1. Purpose of encryption....120
11.1.2. How encryption works....120
11.2. Security of encryption systems....121
11.2.1. Meaning of 'security' in encryption: general observations....121
11.2.2. Absolute security: the one-time pad....122
11.2.3. Relative security at the present state of technology....122
11.2.4. Standardisation and the deliberate restriction of security....123
11.3. The problem of the secure distribution/handover of keys....124
11.3.1. Asymmetric encryption: the public-key process....124
11.3.2. Public-key encryption for private individuals....125
11.3.3. Future processes....125
11.4. Security of encryption products....125
11.5. Encryption in conflict with state interests....126
11.5.1. Attempts to restrict encryption....126
11.5.2. The significance of secure encryption for e-commerce....126
11.5.3. Problems for business travellers....126
11.6. Practical issues in connection with encryption....127

12. The EU's external relations and intelligence gathering....128

12.1. Introduction....128
12.2. Scope for cooperation within the EU....128
12.2.1. Existing cooperation....128
12.2.2. Advantages of a joint European intelligence policy....129
12.2.3. Concluding remarks....129
12.3. Cooperation beyond EU level....129
12.4. Final remarks....131

13. Conclusions and recommendations....132

13.1. Conclusions....132
13.2. Recommendations....135

PROCEDURAL PAGE

At the sitting of 5 July 2000 the European Parliament decided, pursuant to Rule 150(2) of its Rules of Procedure, to set up a Temporary Committee on the ECHELON Interception System and laid down its mandate as outlined in Chapter 1, 1.3. With a view to fulfilling that mandate, at its constituent meeting of 9 July 2000 the Temporary Committee appointed Gerhard Schmid rapporteur.

At its meetings of 29 May, 20 June and 3 July 2001 the committee considered the draft report.

At the last meeting the committee adopted the motion for a resolution by 27 votes to 5, with 2 abstentions.

The following were present for the vote: Carlos Coelho, chairman; Elly Plooij-van Gorsel, Neil MacCormick and Giuseppe Di Lello Finuoli, vice-chairmen; Gerhard Schmid, rapporteur; Mary Elizabeth Banotti, Bastiaan Belder, Maria Berger, Charlotte Cederschiöld, Gérard M.J. Deprez, Giorgos Dimitrakopoulos, Robert J.E. Evans, Colette Flesch, Pernille Frahm, Anna Karamanou, Eva Klamt, Alain Krivine, Torben Lund, Erika Mann, Jean-Charles Marchiani, Hugues Martin, Patricia McKenna, William Francis Newton Dunn (for Jorge Salvador Hernández Mollar), Reino Paasilinna, Bernd Posselt (for Hubert Pirker), Jacques Santer (for Catherine Lalumière), Ilka Schröder, Gary Titley (for Ozan Ceyhun), Maurizio Turco, Gianni Vattimo, W.G. van Velzen, Christian Ulrik von Boetticher, Jan Marinus Wiersma and Christos Zacharakis (for Enrico Ferri).

The minority opinions and the annexes will be published separately (A5-0264/2001-Par2).

The report was tabled on 11 July 2001.

The deadline for tabling amendments will be indicated in the draft agenda for the relevant part-session.

MOTION FOR A RESOLUTION

European Parliament resolution on the existence of a global system for the interception of private and commercial communications (ECHELON interception system) (2001/2098 (INI))

The European Parliament,

– having regard to its decision of 5 July 2000 to set up a Temporary Committee on the ECHELON Interception System and the mandate issued to the Temporary Committee[1],

– having regard to the EC Treaty, one objective of which is the establishment of a common market with a high level of competitiveness,

– having regard to Articles 11 and 12 of the Treaty on European Union, which impose on the Member States a binding requirement to enhance and develop their mutual political solidarity,

– having regard to the Treaty on European Union, in particular Article 6(2) thereof, which lays down the requirement that the EU must respect fundamental rights, and Title V thereof, which sets out provisions governing the common foreign and security policy,

– having regard to Article 12 of the Universal Declaration of Human Rights,

– having regard to the Charter of Fundamental Rights of the EU, Article 7 of which lays down the right to respect for private and family life and explicitly enshrines the right to respect for communications, and Article 8 of which protects personal data,

– having regard to having regard to the European Convention on Human Rights (ECHR), in particular Article 8 thereof, which governs the protection of private life and the confidentiality of correspondence, and the many other international conventions which provide for the protection of privacy,

– having regard to the work carried out by the Temporary Committee on the ECHELON Interception System, which held a large number of hearings and meetings with experts of all kinds, and in particular with senior representatives of the public and private sectors in the sphere of telecommunications and data protection, with employees of intelligence and information services, with journalists, with lawyers with expert knowledge of this area, with members of the national parliaments of the Member States, etc.,

– having regard to Rule 150(2) of its Rules of Procedure,

– having regard to the report of the Temporary Committee on the ECHELON Interception System (A5-0264/2001),

[1] OJ C 121, 24.4.2001, p. 36

The existence of a global system for intercepting private and commercial communications (the ECHELON interception system)

A. whereas the existence of a global system for intercepting communications, operating by means of cooperation proportionate to their capabilities among the USA, the UK, Canada, Australia and New Zealand under the UKUSA Agreement, is no longer in doubt; whereas it seems likely, in view of the evidence and the consistent pattern of statements from a very wide range of individuals and organisations, including American sources, that its name is in fact ECHELON, although this is a relatively minor detail,

B. whereas there can now be no doubt that the purpose of the system is to intercept, at the very least, private and commercial communications, and not military communications, although the analysis carried out in the report has revealed that the technical capabilities of the system are probably not nearly as extensive as some sections of the media had assumed,

C. whereas, therefore, it is surprising, not to say worrying, that many senior Community figures, including European Commissioners, who gave evidence to the Temporary Committee claimed to be unaware of this phenomenon,

The limits of the interception system

D. whereas the surveillance system depends, in particular, upon worldwide interception of satellite communications, although in areas characterised by a high volume of communications only a very small proportion of those communications are transmitted by satellite; whereas this means that the majority of communications cannot be intercepted by earth stations, but only by tapping cables and intercepting radio signals, something which - as the investigations carried out in connection with the report have shown - is possible only to a limited extent; whereas the numbers of personnel required for the final analysis of intercepted communications imposes further restrictions; whereas, therefore, the UKUSA states have access to only a very limited proportion of cable and radio communications and can analyse an even more limited proportion of those communications, and whereas, further, however extensive the resources and capabilities for the interception of communications may be, the extremely high volume of traffic makes exhaustive, detailed monitoring of all communications impossible in practice,

The possible existence of other interception systems

E. whereas the interception of communications is a method of spying commonly employed by intelligence services, so that other states might also operate similar systems, provided that they have the required funds and the right locations; whereas France is the only EU Member State which is – thanks to its overseas territories – geographically and technically capable of operating autonomously a global interception system and also possesses the technical and organisational infrastructure to do so; whereas there is also ample evidence that Russia is likely to operate such a system,

Compatibility with EU law

F. whereas, as regards the question of the compatibility of a system of the ECHELON type with EU law, it is necessary to distinguish between two scenarios: if a system is used purely for intelligence purposes, there is no violation of EU law, since operations in the interests of state security are not subject to the EC Treaty, but would fall under Title V of the Treaty on European Union (CFSP), although at present that title lays down no provisions on the subject, so that no criteria are available; if, on the other hand, the system is misused for the purposes of gathering competitive intelligence, such action is at odds with the Member States' duty of loyalty and with the concept of a common market based on free competition, so that a Member State participating in such a system violates EC law,

G. having regard to the statements made by the Council at the plenary sitting of 30 March 2000 to the effect that 'the Council cannot agree to the creation or existence of a telecommunications interception system which does not comply with the rules laid down in the law of the Member States and which breaches the fundamental principles designed to safeguard human dignity',

Compatibility with the fundamental right to respect for private life (Article 8 of the ECHR)

H. whereas any interception of communications represents serious interference with an individual's exercise of the right to privacy; whereas Article 8 of the ECHR, which guarantees respect for private life, permits interference with the exercise of that right only in the interests of national security, in so far as this is in accordance with domestic law and the provisions in question are generally accessible and lay down under what circumstances, and subject to what conditions, the state may undertake such interference; whereas interference must be proportionate, so that competing interests need to be weighed up and, under the terms of the case law of the European Court of Human Rights, it is not enough that the interference should merely be useful or desirable,

I. whereas an intelligence system which intercepted communications permanently and at random would be in violation of the principle of proportionality and would not be compatible with the ECHR; whereas it would also constitute a violation of the ECHR if the rules governing the surveillance of communications lacked a legal basis, if the rules were not generally accessible or if they were so formulated that their implications for the individual were unforeseeable, or if the interference was not proportionate; whereas most of the rules governing the activities of US intelligence services abroad are classified, so that compliance with the principle of proportionality is at least doubtful and breaches of the principles of accessibility and foreseeability laid down by the European Court of Human Rights probably occur,

J. whereas the Member States cannot circumvent the requirements imposed on them by the ECHR by allowing other countries' intelligence services, which are subject to less stringent legal provisions, to work on their territory, since otherwise the principle of legality, with its twin components of accessibility and foreseeability, would become a dead letter and the case law of the European Court of Human Rights would be deprived of its substance,

K. whereas, in addition, the lawful operations of intelligence services are consistent with fundamental rights only if adequate arrangements exist for monitoring them, in order to counterbalance the risks inherent in secret activities performed by a part of the administrative apparatus; whereas the European Court of Human Rights has expressly stressed the importance of an efficient system for monitoring intelligence operations, so that there are grounds for concern in the fact that some Member States do not have parliamentary monitoring bodies of their own responsible for scrutinising the secret services,

Are EU citizens adequately protected against intelligence services?

L. whereas the protection enjoyed by EU citizens depends on the legal situation in the individual Member States, which varies very substantially, and whereas in some cases parliamentary monitoring bodies do not even exist, so that the degree of protection can hardly be said to be adequate; whereas it is in the fundamental interests of European citizens that their national parliaments should have a specific, formally structured monitoring committee responsible for supervising and scrutinising the activities of the intelligence services; whereas even where monitoring bodies do exist, there is a strong temptation for them to concentrate more on the activities of domestic intelligence services, rather than those of foreign intelligence services, since as a rule it is only the former which affect their own citizens; whereas it would be an encouragement for proportionate interference practices, if intelligence services were obliged to notify a citizen whose communications have been intercepted of this fact afterwards, for instance five years after the interception took place,

M. whereas, in view of their size, satellite receiving stations cannot be built on the territory of a state without its consent,

N. whereas, in the event of cooperation between intelligence services under the CFSP or in the areas of justice and home affairs, the institutions must introduce adequate measures to protect European citizens,

Industrial espionage

O. whereas part of the remit of foreign intelligence services is to gather economic data, such as details of developments in individual sectors of the economy, trends on commodity markets, compliance with economic embargoes, observance of rules on supplying dual-use goods, etc., and whereas, for these reasons, the firms concerned are often subject to surveillance,

P. whereas the US intelligence services do not merely investigate general economic facts but also intercept detailed communications between firms, particularly where contracts are being awarded, and they justify this on the grounds of combating attempted bribery; whereas detailed interception poses the risk that information may be used for the purpose of competitive intelligence-gathering rather than combating corruption, even though the US and the United Kingdom state that they do not do so; whereas, however, the role of the Advocacy Center of the US Department of Commerce is still not totally clear and talks arranged with the Center with a view to clarifying the matter were cancelled,

Q. whereas an agreement on combating the bribery of officials, under which bribery is criminalised at international level, was adopted by the OECD in 1997, and this provides a further reason why individual cases of bribery cannot justify the interception of communications,

R. whereas the situation becomes intolerable when intelligence services allow themselves to be used for the purposes of gathering competitive intelligence by spying on foreign firms with the aim of securing a competitive advantage for firms in the home country, and whereas it is frequently maintained that the global interception system has been used in this way, although no such case has been substantiated,

S. whereas, during the visit by the delegation from the Temporary Committee to the US, authoritative sources confirmed the US Congress Brown Report, indicating that 5% of intelligence gathered via non-open sources is used as economic intelligence; whereas it was estimated by the same sources that this intelligence surveillance could enable US industry to earn up to US$ 7 billion in contracts,

T. whereas sensitive commercial data are mostly kept inside individual firms, so that competitive intelligence-gathering in particular involves efforts to obtain information through members of staff or through people planted in the firm for this purpose or else**,** more and more commonly, by hacking into internal computer networks; whereas only if sensitive data are transmitted externally by cable or radio (satellite) can a communications surveillance system be used for competitive intelligence-gathering; whereas this applies systematically in the following three cases:
- in the case of firms which operate in three time zones, so that interim results are sent from Europe to America and on to Asia;
- in the case of videoconferencing within multinationals using VSAT or cable;
- if vital contracts are being negotiated on the spot (e.g. for the building of plants, telecommunications infrastructure, the creation of new transport systems, etc.) and it is necessary to consult the firm's head office,

U. whereas risk and security awareness in small and medium-sized firms is often inadequate and the dangers of economic espionage and the interception of communications are not recognised,

V. whereas security awareness is not always well developed in the European institutions (with the exception of the European Central Bank, the Council Directorate-General for External Relations and the Commission Directorate-General for External Relations) and action is therefore necessary,

Possible self-protection measures

W. whereas firms can only make themselves secure by safeguarding their entire working environment and protecting all communications channels which are used to send sensitive information; whereas sufficiently secure encryption systems exist at affordable prices on the European market; whereas private individuals should also be urged to encrypt e-mails; whereas an unencrypted e-mail message is like a letter without an envelope; whereas relatively user-friendly systems exist on the Internet which are even made available for private use free of charge,

Cooperation among intelligence services within the EU

X. whereas the EU has reached agreement on the coordination of intelligence-gathering by intelligence services as part of the development of its own security and defence policy, although cooperation with other partners in these areas will continue,

Y. whereas in December 1999 in Helsinki the European Council decided to develop more effective European military capabilities with a view to undertaking the full range of Petersberg tasks in support of the CFSP; whereas the European Council decided furthermore that, in order to achieve this goal, by the year 2003 the Union should be able to deploy rapidly units of about 50 000 – 60 000 troops which should be self-sustaining, including the necessary command, control and intelligence capabilities; whereas the first steps towards such an autonomous intelligence capability have already been taken in the framework of the WEU and the standing Political and Security Committee,

Z. whereas cooperation among intelligence services within the EU seems essential on the grounds that, firstly, a common security policy which did not involve the secret services would not make sense, and, secondly, it would have numerous professional, financial and political advantages; whereas it would also accord better with the idea of the EU as a partner on an equal footing with the United States and could bring together all the Member States in a system which complied fully with the ECHR; whereas the European Parliament would of course have to exercise appropriate monitoring,

AA. whereas the European Parliament is in the process of implementing the regulation on public access to European Parliament, Council and Commission documents by amending the provisions of its Rules of Procedure as regards access to sensitive documents,

Conclusion and amendment of international agreements on the protection of citizens and firms

1. States, on the basis of the information obtained by the Temporary Committee, that the existence of a global system for intercepting communications, operating with the participation of the United States, the United Kingdom, Canada, Australia and New Zealand under the UKUSA Agreement, is no longer in doubt;

2. Calls on the Secretary-General of the Council of Europe to submit to the Ministerial Committee a proposal to protect private life, as guaranteed in Article 8 of the ECHR, brought into line with modern communication and interception methods by means of an additional protocol or, together with the provisions governing data protection, as part of a revision of the Convention on Data Protection, with the proviso that this should neither undermine the level of legal protection established by the European Court of Human Rights nor reduce the flexibility which is vital if future developments are to be taken into account;

3. Calls on the Member States – whose laws governing the interception capabilities of the secret services contain provisions on the protection of privacy which are discriminatory – to provide all European citizens with the same legal guarantees concerning the protection of privacy and the confidentiality of correspondence;

4. Calls on the Member States of the European Union to establish a European platform consisting of representatives of the national bodies that are responsible for monitoring Member States' performance in complying with fundamental and citizens' rights in order to scrutinise the consistency of national laws on the intelligence services with the ECHR and the EU Charter of Fundamental Rights, to review the legal provisions guaranteeing postal and communications secrecy, and, in addition, to reach agreement on a recommendation to the Member States on a Code of Conduct to be drawn up which guarantees all European citizens, throughout the territory of the Member States, protection of privacy as defined in Article 7 of the Charter of Fundamental Rights of the European Union and which, moreover, guarantees that the activities of intelligence services are carried out in a manner consistent with fundamental rights, in keeping with the conditions set out in Chapter 8 of this report, and in particular Section 8.3.4., as derived from Article 8 of the ECHR;

5. Calls on the Member States to adopt the EU Charter of Fundamental Rights as a legally binding and enforceable act at the next Intergovernmental Conference in order to raise the standard of protection for fundamental rights, particularly with regard to the protection of privacy;

6. Calls on the member countries of the Council of Europe to adopt an additional protocol which enables the European Communities to accede to the ECHR or to consider other measures designed to prevent disputes relating to case law arising between the European Court of Human Rights and the Court of Justice of the European Communities;

7. Urges the EU institutions in the meantime to apply the fundamental rights enshrined in the Charter within the scope of their respective powers and activities;

8. Calls on the UN Secretary-General to instruct the competent committee to put forward proposals designed to bring Article 17 of the International Covenant on Civil and Political Rights, which guarantees the protection of privacy, into line with technical innovations;

9. Regards it as essential that an agreement should be negotiated and signed between the European Union and the United States stipulating that each of the two parties should observe, vis-à-vis the other, the provisions governing the protection of the privacy of citizens and the confidentiality of business communications applicable to its own citizens and firms;

10. Calls on the USA to sign the Additional Protocol to the International Covenant on Civil and Political Rights, so that complaints by individuals concerning breaches of the Covenant by the USA can be submitted to the Human Rights Committee set up under the Covenant; calls on the relevant American NGOs, in particular the ACLU (American Civil Liberties Union) and the EPIC (Electronic Privacy Information Center), to exert pressure on the US Administration to that end;

National legislative measures to protect citizens and firms

11. Urges the Member States to review and if necessary to adapt their own legislation on the operations of the intelligence services to ensure that it is consistent with fundamental rights as laid down in the ECHR and with the case law of the European Court of Human Rights;

12. Calls on the Member States to endow themselves with binding instruments which afford natural and legal persons effective protection against all forms of illegal interception of their communications;

13. Calls on the Member States to aspire to a common level of protection against intelligence operations and, to that end, to draw up a Code of Conduct (as referred to in paragraph 4) based on the highest level of protection which exists in any Member State, since as a rule it is citizens of other states, and hence also of other Member States, that are affected by the operations of foreign intelligence services;

14. Calls on the Member States to negotiate with the USA a Code of Conduct similar to that of the EU;

15. Calls on those Member States which have not yet done so to guarantee appropriate parliamentary and legal supervision of their secret services;

16. Urges the Council and the Member States to establish as a matter of priority a system for the democratic monitoring and control of the autonomous European intelligence capability and other joint and coordinated intelligence activities at European level; proposes that the European Parliament should play an important role in this monitoring and control system;

17. Calls on the Member States to pool their communications interception resources with a view to enhancing the effectiveness of the CFSP in the areas of intelligence-gathering and the fight against terrorism, nuclear proliferation or international drug trafficking, in accordance with the provisions governing the protection of citizens' privacy and the confidentiality of business communications, and subject to monitoring by the European Parliament, the Council and the Commission;

18. Calls on the Member States to conclude an agreement with third countries aimed at providing increased protection of privacy for EU citizens, under which all contracting states give a commitment, where one contracting state intercepts communications in another contracting state, to inform the latter of the planned actions;

Specific legal measures to combat industrial espionage

19. Calls on the Member States to consider to what extent industrial espionage and the payment of bribes as a way of securing contracts can be combated by means of European and international legal provisions and, in particular, whether WTO rules could be adopted which take account of the distortions of competition brought about by such practices, for example by rendering contracts obtained in this way null and void; calls on the United States, Australia, New Zealand and Canada to join this initiative;

20. Calls on the Member States to undertake to incorporate in the EC Treaty a clause prohibiting industrial espionage and not to engage in industrial espionage against one another, either directly or with the assistance of a foreign power which might carry out operations on their territory, nor to allow a foreign power to conduct espionage operations from the soil of an EU Member State, thereby complying with the letter and spirit of the EC Treaty;

21. Calls on the Member States to undertake by means of a clear and binding instrument not to engage in industrial espionage, thereby signifying their compliance with the letter and spirit of the EC Treaty; calls on the Member States to transpose this binding principle into their national legislation on intelligence services;

22. Calls on the Member States and the US Administration to start an open US-EU dialogue on economic intelligence-gathering;

Measures concerning the implementation of the law and the monitoring of that implementation

23. Calls on the national parliaments which have no parliamentary monitoring body responsible for scrutinising the activities of the intelligence services to set up such a body;

24. Calls on the monitoring bodies responsible for scrutinising the activities of the secret services, when exercising their monitoring powers, to attach great importance to the protection of privacy, regardless of whether the individuals concerned are their own nationals, other EU nationals or third-country nationals;

25. Calls on the Member States to make sure that their intelligence systems are not misused for the purposes of gathering competitive intelligence, an act at odds with the Member States' duty of loyalty and with concept of a common market based on free competition;

26. Calls on Germany and the United Kingdom to make the authorisation of further communications interception operations by US intelligence services on their territory conditional on their compliance with the ECHR, i.e. to stipulate that they should be consistent with the principle of proportionality, that their legal basis should be accessible and that the implications for individuals should be foreseeable, and to introduce corresponding, effective monitoring measures, since they are responsible for ensuring that intelligence operations authorised or even merely tolerated on their territory respect human rights;

Measures to encourage self-protection by citizens and firms

27. Calls on the Commission and the Member States to inform their citizens and firms about the possibility that their international communications may, under certain circumstances, be intercepted; insists that this information should be accompanied by practical assistance in designing and implementing comprehensive protection measures, including the security of information technology;

28. Calls on the Commission, the Council and the Member States to develop and implement an effective and active policy for security in the information society; insists that as part of this policy specific attention should be given to increasing the awareness of all users of modern communication systems of the need to protect confidential information; furthermore, insists on the establishment of a Europe-wide, coordinated network of agencies capable of providing practical assistance in designing and implementing comprehensive protection strategies;

29. Urges the Commission and Member States to devise appropriate measures to promote, develop and manufacture European encryption technology and software and above all to support projects aimed at developing user-friendly open-source encryption software;

30. Calls on the Commission and Member States to promote software projects whose source text is made public (open-source software), as this is the only way of guaranteeing that no backdoors are built into programmes;

31. Calls on the Commission to lay down a standard for the level of security of e-mail software packages, placing those packages whose source code has not been made public in the 'least reliable' category;

32. Calls on the European institutions and the public administrations of the Member States systematically to encrypt e-mails, so that ultimately encryption becomes the norm;

33. Calls on the Community institutions and the public administrations of the Member States to provide training for their staff and make their staff familiar with new encryption technologies and techniques by means of the necessary practical training and courses;

34. Calls for particular attention to be paid to the position of the applicant countries; urges that they should be given support, if their lack of technological independence prevents them from implementing the requisite protective measures;

Other measures

35. Calls on firms to cooperate more closely with counter-espionage services, and particularly to inform them of attacks from outside for the purposes of industrial espionage, in order to improve the services' efficiency;

36. Instructs the Commission to have a security analysis carried out which will show what needs to be protected, and to have a protection strategy drawn up;

37. Calls on the Commission to update its encryption system in line with the latest developments, given that modernisation is urgently needed, and calls on the budgetary authorities (the Council together with Parliament) to provide the necessary funding;

38. Requests the competent committee to draw up an own-initiative report on security and the protection of secrecy in the European institutions;

39. Calls on the Commission to ensure that data is protected in its own data-processing systems and to step up the protection of secrecy in relation to documents not accessible to the public;

40. Calls on the Commission and the Member States to invest in new technologies in the field of decryption and encryption techniques as part of the Sixth Research Framework Programme;

41. Urges states which have been placed at a disadvantage by distortions of competition resulting from state aid or the economic misuse of espionage to inform the authorities and monitoring bodies of the state from which the activities were undertaken in order to put a stop to the distorting activities;

42. Calls on the Commission to put forward a proposal to establish, in close cooperation with industry and the Member States, a Europe-wide, coordinated network of advisory centres - in particular in those Member States where such centres do not yet exist - to deal with issues relating to the security of the information held by firms, with the twin task of increasing awareness of the problem and providing practical assistance;

43. Takes the view that an international congress on the protection of privacy against telecommunications surveillance should be held in order to provide NGOs from Europe, the USA and other countries with a forum for discussion of the cross-border and international aspects of the problem and coordination of areas of activity and action;

44. Instructs its President to forward this resolution to the Council, the Commission, the Secretary-General and Parliamentary Assembly of the Council of Europe and the governments and parliaments of the Member States and applicant countries, the United States, Australia, New Zealand and Canada.

EXPLANATORY STATEMENT

1. Introduction

1.1. The reasons for setting up the committee

On 5 July 2000 the European Parliament decided to set up a temporary committee on the ECHELON system. This step was prompted by the debate on the study commissioned by STOA[2] concerning the so-called ECHELON system[3], which the author, Duncan Campbell, had presented at a hearing of the Committee on Citizens' Freedoms and Rights, Justice and Home Affairs on the subject 'the European Union and data protection'.

1.2. The claims made in the two STOA studies on a global interception system codenamed ECHELON

1.2.1. The first STOA report of 1997

A report which STOA commissioned from the Omega Foundation for the European Parliament in 1997 on 'An Appraisal of Technologies of Political Control' described ECHELON in a chapter concerning 'national and international communications interception networks'. The author claimed that all e-mail, telephone and fax communications in Europe were routinely intercepted by the US National Security Agency[4]. As a result of this report, the alleged existence of a comprehensive global interception system called ECHELON was brought to the attention of people throughout Europe.

1.2.2. The 1999 STOA reports

In 1999, in order to find out more about this subject, STOA commissioned a five-part study of the 'development of surveillance technology and risk of abuse of economic information'. Part 2/5, by Duncan Campbell, concerned the existing intelligence capacities and particularly the mode of operation of ECHELON[5].

[2] STOA (Scientific and Technological Options Assessment) is a department of the Directorate-General for Research of the European Parliament which commissions research at the request of committees. However, the documents it produces are not subject to scientific review.

[3] *Duncan Campbell*, The state of the art in Communications Intelligence (COMINT) of automated processing for intelligence purposes of intercepted broadband multi-language leased or common carrier systems and its applicability to COMINT targeting and selection, including speech recognition, Part 2/5, in: STOA (Ed.), Development of Surveillance Technology and Risk of Abuse of Economic Information (October 1999), PE 168.184.

[4] *Steve Wright,* An appraisal of technologies of political control, STOA interim study, PE 166.499/INT.ST. (1998), 20

[5] *Duncan Campbell*, The state of the art in Communications Intelligence (COMINT) of automated processing for intelligence purposes of intercepted broadband multi-language leased or common carrier systems and its applicability to COMINT targeting and selection, including speech recognition, Part 2/5, in: STOA (Ed.), Development of Surveillance Technology and Risk of Abuse of Economic Information (October 1999), PE 168.184.

Concern was aroused in particular by the assertion in the report that ECHELON had moved away from its original purpose of defence against the Eastern Bloc and was currently being used for purposes of industrial espionage. Examples of alleged industrial espionage were given in support of the claim: in particular, it was stated that Airbus and Thomson CFS had been damaged as a result. Campbell bases his claims on reports in the American press[6]

As a result of the STOA study, ECHELON was debated in the parliaments of virtually all the Member States; in France and Belgium, reports were even drafted on it.

1.3. The mandate of the committee

At the same time as it decided to set up a temporary committee, the European Parliament drew up its mandate[7]. It reads as follows:

- '- to verify the existence of the communications interception system known as ECHELON, whose operation is described in the STOA report published under the title "Development of surveillance technology and risks of abuse of economic information";
- - to assess the compatibility of such a system with Community law, in particular Article 286 of the EC Treaty and Directives 95/46/EC and 97/66/EC, and with Article 6(2) of the EU Treaty, in the light of the following questions:
    - - are the rights of European citizens protected against activities of secret services?
    - - is encryption an adequate and sufficient protection to guarantee citizens' privacy or should additional measures be taken and if so what kind of measures?
    - - how can the EU institutions be made better aware of the risks posed by these activities and what measures can be taken?
- - to ascertain whether European industry is put at risk by the global interception of communications;
- - possibly, to make proposals for political and legislative initiatives.'

1.4. Why not a committee of inquiry?

The European Parliament decided to set up a temporary committee because a committee of inquiry can be set up only to investigate violations of Community law under the EC Treaty (Article 193 TEC), and such committees can accordingly only consider matters governed by it. Matters falling under Titles V (Common Foreign and Security Policy) and VI (Police and Judicial Cooperation in Criminal Matters) of the Treaty on European Union are excluded. Moreover, under the interinstitutional decision[8] the special powers of a committee of inquiry to call people to appear and to inspect documents apply only if grounds of secrecy or public or national security do not dictate otherwise, which would certainly make it impossible to summon secret services to appear. Furthermore, a committee of inquiry cannot extend its work to third countries, because by definition the latter cannot violate EU law. Thus, setting up a committee of inquiry would only have restricted the scope of any investigations opening up any additional

[6] Raytheon Corp Press release, http://www.raytheon.com/sivam/contract.html; *Scott Shane, Tom Bowman*, America's Fortress of Spies, Baltimore Sun, 3.12.1995
[7] European Parliament decision of 5 July 2000, B5-0593/2000, OJ C 121/131 of 24 April 2001.
[8] Decision of the European Parliament, the Council and the Commission of 19 April 1995 on the detailed provisions governing the exercise of the European Parliament's right of inquiry (95/167/EC), Article 3(3)-(5).

rights, for which reason the idea was rejected by a majority of Members of the European Parliament.

1.5. Working method and schedule

With a view to carrying out its mandate in full, the committee decided to proceed in the following way. A programme of work proposed by the rapporteur and adopted by the committee listed the following relevant topics: 1. Certain knowledge about ECHELON, 2. Debate by national parliaments and governments, 3. Intelligence services and their operations, 4. Communications systems and the scope for intercepting them, 5. Encryption, 6. Industrial espionage, 7. Aims of espionage and protective measures, 8. Legal context and protection of privacy and 9. Implications for the EU's external relations. The topics were considered consecutively at the individual meetings, the order of consideration being based on practical grounds and thus not implying anything about the value assigned to the individual topics. By way of preparation for the meetings, the rapporteur systematically scrutinised and evaluated the material available. At the meetings, in accordance with the requirements of the topic concerned, representatives of national administrations (particularly secret services) and parliaments in their capacity as bodies responsible for monitoring secret services were invited to attend, as were legal experts and experts in the fields of communications and interception technology, business security and encryption technology with both academic and practical backgrounds. Journalists who had investigated this field were also heard. The meetings were generally held in public, although some sessions were also held behind closed doors where this was felt to be advisable in the interests of obtaining information. In addition, the chairman of the committee and the rapporteur visited London and Paris together to meet people who for a wide variety of different reasons were unable to attend meetings of the committee but whose involvement in the committee's work nonetheless seemed advisable. For the same reasons, the committee's bureau, the coordinators and the rapporteur travelled to the USA. The rapporteur also held many one-to-one talks, in some cases in confidence.

1.6. Characteristics ascribed to the ECHELON system

The system known as 'ECHELON' is an interception system which differs from other intelligence systems in that it possesses two features which make it quite unusual:

The first such feature attributed to it is the capacity to carry out quasi-total surveillance. Satellite receiver stations and spy satellites in particular are alleged to give it the ability to intercept any telephone, fax, Internet or e-mail message sent by any individual and thus to inspect its contents.

The second unusual feature of ECHELON is said to be that the system operates worldwide on the basis of cooperation proportionate to their capabilities among several states (the UK, the USA, Canada, Australia and New Zealand), giving it an added value in comparison to national systems: the states participating in ECHELON (UKUSA states[9]) can place their interception systems at each other's disposal, share the cost and make joint use of the resulting information. This type of international cooperation is essential in particular for the worldwide interception of satellite communications, since only in this way is it possible to ensure in international communications that both sides of a dialogue can be intercepted. It is clear that, in view of its

[9] See Chapter 5, 5.4.

size, a satellite receiver station cannot be established on the territory of a state without that state's knowledge. Mutual agreement and proportionate cooperation among several states in different parts of the world is essential.

Possible threats to privacy and to businesses posed by a system of the ECHELON type arise not only from the fact that is a particularly powerful monitoring system, but also that it operates in a largely legislation-free area. Systems for the interception of international communications are not usually targeted at residents of the home country. The person whose messages were intercepted would have no domestic legal protection, not being resident in the country concerned. Such a person would be completely at the mercy of the system. Parliamentary supervision would also be inadequate in this area, since the voters, who assume that interception 'only' affects people abroad, would not be particularly interested in it, and elected representatives chiefly follow the interests of their voters. That being so, it is hardly surprising that the hearings held in the US Congress concerning the activities of the NSA were confined to the question of whether US citizens were affected by it, with no real concern expressed regarding the existence of such a system in itself. It thus seems all the more important to investigate this issue at European level.

2. The operations of foreign intelligence services

2.1. Introduction

In addition to police forces, most governments run intelligence services to protect their country's security. As their operations are generally secret, they are also referred to as secret services. These services have the following tasks:

- gathering information to avert dangers to state security
- counter-espionage in general
- averting possible dangers to the armed forces
- gathering information about situations abroad.

2.2. What is espionage?

Governments have a need for systematic collection and evaluation of information about certain situations in other states. This serves as a basis for decisions concerning the armed forces, foreign policy and so on. They therefore maintain foreign intelligence services, part of whose task is to systematically assess information available from public sources. The rapporteur has been informed that on average this accounts for at least 80% of the work of the intelligence services.[10] However, particularly significant information in the fields concerned is kept secret from governments or businesses and is therefore not publicly accessible. Anyone who nonetheless wishes to obtain it has to steal it. Espionage is simply the organised theft of information.

2.3. Espionage targets

The classic targets of espionage are military secrets, other government secrets or information concerning the stability of or dangers to governments. These may for example comprise new weapons systems, military strategies or information about the stationing of troops. No less important is information about forthcoming decisions in the fields of foreign policy, monetary decisions or inside information about tensions within a government. In addition there is also interest in economically significant information. This may include not only information about sectors of the economy but also details of new technologies or foreign transactions.

2.4. Espionage methods

Espionage involves gaining access to information which the holder would rather protect from being accessed by outsiders. This means that the protection needs to be overcome and penetrated. This is the case with both political and industrial espionage. Thus the same problems arise with espionage in both fields, and the same techniques are accordingly used in both of them. Logically speaking there is no difference, only the level of protection is generally lower in the economic sphere, which sometimes makes it easier to carry out industrial espionage. In

[10] The Commission on the Roles and Capabilities of the US Intelligence Community has stated in its report 'Preparing for the 21st Century: An Appraisal of US Intelligence' (1996) that 95% of all economic intelligence is derived from open sources (Chapter 2, 'The Role of Intelligence').
http://www.gpo/int/report.html

particular, businessmen tend to be less aware of risks when using interceptible communication media than does the state when employing them in fields where security is a concern.

2.4.1. Human intelligence

Protection of secret information is always organised in the same way:
- only a small number of people, who have been vetted, have access to secret information
- there are established rules for dealing with such information
- normally the information does not leave the protected area, and if it does so, it leaves only in a secure manner or encrypted form. The prime method of carrying out organised espionage is therefore by gaining access to the desired information directly through **people** ('human intelligence'). These may be:
  - plants (agents) acting on behalf of the service/business engaging in espionage
  - people recruited from the target area.

Recruits generally work for an outside service or business for the following reasons:
- sexual seduction
- bribery in cash or in kind
- blackmail
- ideological grounds
- attachment of special significance or honour to a given action (playing on dissatisfaction or feelings of inferiority).

A borderline case is unintentional cooperation by means of which information is 'creamed off'. This involves persuading employees of authorities or businesses to disclose information in casual conversation, for example by exploiting their vanity, under apparently harmless circumstances (through informal contact at conferences or trade fairs or in hotel bars).

The use of people has the advantage of affording direct access to the desired information. However, there are also disadvantages:
- counter-espionage always concentrates on people or controlling agents
- where an organisation's staff are recruited, the weaknesses which laid them open to recruitment may rebound on the recruiting body
- people always make mistakes, which means that sooner or later they will be detected through counter-espionage operations.

Where possible, therefore, organisations try to replace the use of agents or recruits with non-human espionage. This is easiest in the case of the analysis of radio signals from military establishments or vehicles.

2.4.2. Processing of electromagnetic signals

The form of espionage by technical means with which the public are most familiar is that which uses satellite photography. In addition, however, electromagnetic signals of any kind are intercepted and analysed ('signals intelligence', SIGINT).

2.4.2.1. Electromagnetic signals used for non-communication purposes

In the military field, certain electromagnetic signals, e.g. those from radar stations, may provide valuable information about the organisation of enemy air defences ('electronic intelligence', ELINT). In addition, electromagnetic radiation which could reveal details of the position of troops, aircraft, ships or submarines is a valuable source of information for an intelligence service. Monitoring other states' spy satellites which take photographs, and recording and decoding signals from such satellites, is also useful.
The signals are recorded by ground stations, from low-orbit satellites or from quasi-geostationary SIGINT satellites. This aspect of intelligence operations using electromagnetic means consumes a large part of services' interception capacity. However, this is not the only use made of technology.

2.4.2.2. Processing of intercepted communications

The foreign intelligence services of many states intercept the military and diplomatic communications of other states. Many of these services also monitor the civil communications of other states if they have access to them. In some states, services are also authorised to monitor incoming or outgoing communications in their own country. In democracies, intelligence services' monitoring of the communications of the country's **own** citizens is subject to certain triggering conditions and controls. However, domestic law in general only protects nationals within the territory of their own country and other residents of the country concerned (see Chapter 8).

2.5. The operations of certain intelligence services

Public debate has been sparked primarily by the interception operations of the US and British intelligence services. They have been criticised for recording and analysing communications (voice, fax, e-mail). A **political** assessment requires a yardstick for judging such operations. The interception operations of foreign intelligence services in the EU may be taken as a basis for comparison. Table 1 provides an overview. This shows that interception of private communications by foreign intelligence services is by no means confined to the US or British foreign intelligence services.

Country	Communications in foreign countries	State communications	Civilian communications
Belgium	+	+	-
Denmark	+	+	+
Finland	+	+	+

France	+	+	+
Germany	+	+	+
Greece	+	+	-
Ireland	-	-	-
Italy	+	+	+
Luxembourg	-	-	-
Netherlands	+	+	+
Austria	+	+	-
Portugal	+	+	-
Sweden	+	+	+
Spain	+	+	+
UK	+	+	+
USA	+	+	+
Canada	+	+	+
Australia	+	+	+
New Zealand	+	+	+

Table 1: Interception operations by intelligence services in the EU and in the UKUSA states

The columns refer to:

Column 1: The country concerned

Column 2: Foreign Communications; all incoming and outgoing civilian, military or diplomatic communications[11]

Column 3: State communications (military, embassies, etc.)

Column 4: Civilian communications

[1]+[1] signifies that communications are intercepted
[1]-[1] signifies that communications are not intercepted

[11] If the intelligence service has access to the relevant cables, it can intercept both incoming and outgoing communications. If the intelligence service targets satellite communications, it has access only to the downlink, but can intercept all the communications it carries, including those not intended for its own territory. Since as a rule the satellite footprints cover the whole of Europe or an even wider area (see Chapter 4, 4.2.5.), satellite communications throughout Europe can be intercepted using receiving stations in one European country.

3. Technical conditions governing the interception of telecommunications

3.1. The interceptibility of various communication media

If people wish to communicate with one another over a given distance, they need a medium. This medium may be:

- air (sound waves)
- light (Morse lamp, fibreoptic cable)
- electric current (telegraph, telephone)
- an electromagnetic wave (all forms of radio).

Any third party who succeeds in accessing the medium can intercept the communications. This process may be easy or difficult, feasible anywhere or only from certain locations. Two extreme cases are discussed below: the technical possibilities available to a spy working on the spot, on the one hand, and the scope for a worldwide interception system, on the other.

3.2. The scope for interception on the spot[12]

On the spot, any form of communication can be intercepted if the eavesdropper is prepared to break the law and the target does not take protective measures.

- **Conversations** in rooms can be intercepted by means of planted microphones (bugs) or laser equipment which picks up vibrations in window panes.

- **Screens** emit radiation which can be picked up at a distance of up to 30 metres, revealing the information on the screen.

- **Telephone, fax, and e-mail messages** can be intercepted if the eavesdropper taps into a cable leaving the relevant building.

- Although the infrastructure required is costly and complex, communications from a **mobile phone** can be intercepted if the interception station is situated in the same radio cell (diameter 300 m in urban areas, 30 km in the countryside).

- **Closed-circuit communications** can be intercepted within the USW-radio range.

Conditions for the use of espionage equipment are ideal on the spot, since the interception measures can be focused on one person or one target and almost every communication can be intercepted. The only disadvantage may be the risk of detection in connection with the planting of bugs or the tapping of cables.

[12] *Manfred Fink*, Eavesdropping on the economy – Interception risks and techniques – prevention and protection, Richard Boorberg Verlag (1996).

3.3. The scope for a worldwide interception system

Today, various media are available for all forms of intercontinental communication (voice, fax and data). The scope for a worldwide interception system is restricted by two factors:

- restricted access to the communication medium
- the need to filter out the relevant communication from a huge mass of communications taking place at the same time.

3.3.1. Access to communication media

3.3.1.1. Cable communications

All forms of communication (voice, fax, e-mail, data) are transmitted by cable. Access to the cable is a prerequisite for the interception of communications of this kind. Access is certainly possible if the terminal of a cable connection is situated on the territory of a state which allows interception. **In technical terms**, therefore, within an individual state all communications carried by cable can be intercepted, provided this is permissible under the law. However, foreign intelligence services generally have no legal access to cables situated on the territory of other states. At best, they can gain illegal access to a specific cable, although the risk of detection is high.

From the telegraph age onwards, intercontinental cable connections have been achieved by means of underwater cables. Access to these cables is always possible at those points where they emerge from the water. If several states join forces to intercept communications, access is possible to all the terminals of the cable connections situated in those states. This was historically significant, since both the underwater telegraph cables and the first underwater coaxial telephone cables linking Europe and America landed in Newfoundland and the connections to Asia ran via Australia, because regenerators were required. Today, fibreoptic cables follow the direct route, regardless of the mountainous nature of the ocean bed and the need for regenerators, and do not pass via Australia or New Zealand.

Electric cables may also be tapped between the terminals of a connection, by means of induction (i.e. electromagnetically, by attaching a coil to the cable), without creating a direct, conductive connection. Underwater electric cables can also be tapped in this way from submarines, albeit at very high cost. This technique was employed by the USA in order to tap into a particular underwater cable laid by the USSR to transmit unencrypted commands to Soviet atomic submarines. The high costs alone rule out the comprehensive use of this technique.

In the case of the older-generation fibreoptic cables used today, inductive tapping is only possible at the regenerators. These regenerators transform the optical signal into an electrical signal, strengthen it and then transform it back into an optical signal. However, this raises the issue of how the enormous volumes of data carried on a cable of this kind can be transmitted from the point of interception to the point of evaluation without the laying of a separate fibreoptic cable. On cost grounds, the use of a submarine fitted with processing equipment is conceivable only in very rare cases, for example in wartime, with a view to intercepting the enemy's strategic military communications. In your rapporteur's view, the use of submarines for

the routine surveillance of international telephone traffic can be ruled out. The new-generation fibreoptic cables use erbium lasers as regenerators – interception by means of electromagnetic coupling is thus no longer possible! Communications transmitted using fibreoptic cables of this kind can thus only be intercepted at the terminals of the connection.

The practical implication for the UKUSA states (the alliance formed for the purposes of interception) is that communications can be intercepted at acceptable cost only at the terminals of the underwater cables which land on their territory. Essentially, therefore, they can only tap incoming or outgoing cable communications! In other words, their access to cable communications **in Europe** is restricted to **the territory of the United Kingdom**, since hitherto internal communications have mostly been transmitted via the domestic cable network. The privatisation of telecommunications may give rise to exceptions, but these are specific and unpredictable!

This is valid at least for telephone and fax communications. Other conditions apply to communications transmitted over the Internet via cable. The situation can be summarised as follows:

- Internet communications are carried out using data packets and different packets addressed to the same recipient may take different routes through the network.

- At the start of the Internet age, spare capacity in the public network was used for the transmission of e-mail communications. For that reason, the routes followed by individual data packets were completely unpredictable and arbitrary. At that time, the most important international connection was the 'science backbone' between Europe and America.

- The commercialisation of the Internet and the establishment of Internet providers also resulted in a commercialisation of the network. Internet providers operated or rented their own networks. They therefore made increasing efforts to keep communications within their own network in order to avoid paying user fees to other operators. Today, the route taken through the network by a data packet is therefore not solely determined by the capacity available on the network, but also hinges on costs considerations.

- An e-mail sent from a client of one provider to a client of another provider is generally routed through the firm's network, even if this is not the quickest route. Routers, computers situated at network junctions and which determine the route by which data packets will be transmitted, organise the transition to other networks at points known as switches.

- At the time of the science backbone, the switches for the routing of global Internet communications were situated in the USA. For that reason, at that time intelligence services could intercept a substantial proportion of European Internet communications. Today, only a small proportion of intra-European Internet communications are routed via the USA[13].

[13] With the aid of a demonstration version of Visual Route, a programme which reveals the route taken by an Internet link, it was shown that a link from Germany to England, Finland or Greece passes via the USA and the UK. A link from Germany to France likewise passes via the UK. Links from Luxembourg to Belgium, Greece, Sweden or Portugal pass via the USA, and to Germany, Finland, France, Italy, the Netherlands or Austria via the switch in London. http://visualroute.cgan.com.hk/

- A small proportion of intra-European communications are routed via a switch in London to which, since foreign communications are involved, the British monitoring station GCHQ has access. The majority of communications do not leave the continent: for example, more than 95% of intra-German Internet communications are routed via a switch in Frankfurt.

In practical terms, this means that the **UKUSA states** have access only to **a very limited proportion** of Internet communications transmitted by cable.

3.3.1.2. Radio communications[14]

The interceptibility of radio communications depends on the range of the electromagnetic waves employed. If the radio waves run along the surface of the earth (so-called **ground waves**), their range is restricted and is determined by the topography of the earth's surface, the degree to which it is built up and the amount of vegetation. If the radio waves are transmitted towards space (so-called **space waves**), two points a substantial distance apart can be linked by means of the reflection of the sky wave from layers of the ionosphere. Multiple reflections substantially increase the range.

The range is determined by the wavelength:

- Very long and long waves (3 kHz – 300 kHz) propagate only via ground waves, because space waves are not reflected. They have very short ranges.

- Medium waves (300 kHz – 3 MHz) propagate via ground waves and at night also via space waves. They are medium-range radio waves.

- Short waves (3 MHz – 30 MHz) propagate primarily via ground waves; multiple reflections make **worldwide** reception possible.

- Ultra-short waves (30 MHz – 300 MHz) propagate only via ground waves, because space waves are not reflected. They propagate in a relatively straight line, like light, with the result that, because of the curvature of the earth, their range is determined by the height of the transmitting and receiving antennae. Depending on power, they have ranges of up to 100 km (roughly 30 km in the case of mobile phones).

- Decimetre and centimetre waves (30 MHz – 30 GHz) propagate in a manner even more akin to light than ultra-short waves. They are easy to focus, clearing the way for low-power, unidirectional transmissions (ground-based microwave radio links). They can only be received by antennae situated almost or exactly in line-of-sight.

Long and medium waves are used only for radio transmitters, radio beacons, etc. Short wave and above all, USW and decimetre/centimetre waves are used for military and civil radio communications.

[14] *Ulrich Freyer*, Message transmission technology, Hanser Verlag (2000).

The details outlined above show that a global communications interception system can only intercept short-wave radio transmissions. In the case of all other types of radio transmission, the interception station must be situated within a 100 km radius (e.g. on a ship, in an embassy).

The practical implication for the **UKUSA states** with terrestrial listening stations is that they can intercept only a very limited proportion of radio communications.

3.3.1.3. Communications transmitted by geostationary telecommunications satellites[15]

As already referred to above, decimetre and centimetre waves can very easily be focused to form microwave radio links. If a microwave radio link is set up transmitting to a telecommunications satellite in a high, geostationary orbit and the satellite receives the microwave signals, converts them and transmits them back to earth, large distances can be covered without the use of cables. The range of such a link is essentially restricted only by the fact that the satellite can receive and transmit only in a straight line. For that reason, several satellites are employed to provide worldwide coverage (for more details, see Chapter 4). If **UKUSA States** operate listening stations in the relevant regions of the earth, in principle they can intercept all telephone, fax and data traffic transmitted via such satellites.

3.3.1.4. Scope for interception from aircraft and ships

It has long been known that special AWACS aircraft are used for the purpose of locating other aircraft over long distances. The radar equipment in these aircraft works in conjunction with a detection system, designed to identify specific objectives, which can locate forms of electronic radiation, classify them and correlate them with radar sightings .They have no separate SIGINT capability[16]. In contrast, the slow-flying EP-3 spy plane used by the US Navy has the capability to intercept microwave, USW and short-wave transmissions. The signals are analysed directly on board and the aircraft is used solely for military purposes[17].

In addition, surface ships, and in coastal regions, submarines are used to intercept military radio transmissions[18].

3.3.1.5. The scope for interception by spy satellites

Provided they are not focused through the use of appropriate antennae, radio waves radiate in all directions, i.e. also into space. Low-orbit Signals Intelligence Satellites can only lock on to the target transmitter for a few minutes in each orbit. In densely populated, highly industrialised areas interception is hampered to such a degree by the high density of transmitters using similar frequencies that it is virtually impossible to filter out individual signals[19]. The satellites cannot be used for the continuous monitoring of civilian radio communications.

[15] *Hans Dodel*, Satellite communications, Hüthig Verlag (1999).
[16] Letter from the Minister of State in the German Federal Defence Ministry, Walter Kolbow, to the rapporteur, dated 14 February 2001.
[17] Süddeutsche Zeitung No 80, 5.4.2001, 6.
[18] *Jeffrey T. Richelson*, The U.S. Intelligence Community (1989), 188, 190.
[19] Letter from the Minister of State in the German Federal Defence Ministry, Walter Kolbow, to the rapporteur, dated 14 February 2001.

Alongside these satellites, the USA operates so-called quasi-geostationary SIGINT satellites stationed in a high earth orbit (42 000 km)[20]. Unlike the geostationary telecommunications satellites, these satellites have an inclination of between 3 and 10°, an apogee of between 39 000 and 42 000 km, and a perigee of between 30 000 and 33 000 km. The satellites are thus not motionless in orbit, but move in a complex elliptical orbit, which enables them to cover a larger area of the earth in the course of one day and to locate sources of radio transmissions. This fact, and the other non-classified characteristics of the satellites, point to their use for purely military purposes.

The signals received are transmitted to the receiving station by means of a strongly-focused, 24 GHz downlink.

3.3.2. Scope for the automatic analysis of intercepted communications: the use of filters

When foreign communications are intercepted, no single telephone connection is monitored on a targeted basis. Instead, some or all of the communications transmitted via the satellite or cable in question are tapped and filtered by computers employing keywords – analysis of every single communication would be completely impossible.

It is easy to filter communications transmitted along a given connection. Specific faxes and e-mails can also be singled out through the use of keywords. If the system has been trained to recognise a particular voice, communications involving that voice can be singled out[21]. However, according to the information available to the rapporteur the automatic recognition to a sufficient degree of accuracy of words spoken by any voice is not yet possible. Moreover, the scope for filtering out is restricted by other factors: the ultimate capacity of the computers, the language problem and, above all, the limited number of analysts who can read and assess filtered messages.

When assessing the capabilities of filter systems, consideration must also be given to the fact that in the case of an interception system working on the basis of the 'vacuum-cleaner principle' those technical capabilities are spread across a range of topics. Some of the keywords relate to military security, some to drug trafficking and other forms of international crime, some to the trade in dual-use goods and some to compliance with embargoes. Some of the keywords also relate to economic activities. Any move to narrow down the range of keywords to economically interesting areas would simply run counter to the demands made on intelligence services by governments; what is more, even the end of the Cold War was not enough to prompt such a step[22].

3.3.3. The example of the German Federal Intelligence Service

Department 2 of the German Federal Intelligence Service (FIS) obtains information through the interception of foreign communications. This activity was the subject of a review by the German Federal Constitutional Court. The details made public during the court proceedings[23], combined with the evidence given to the Temporary Committee on 21 November 2000 by Mr Ernst

[20] Major *A. Andronov*, Zarubezhnoye voyennoye obozreniye, No 12, 1993, 37-43.
[21] Information supplied privately to the rapporteur (source protected).
[22] Information supplied privately to the rapporteur (source protected).
[23] BverfG, 1 BvR 2226/94, 14 July 1999, paragraph 1.

Uhrlau, the coordinator for the secret services in the Federal Chancellor's Office, give an insight into the scope for obtaining intelligence by intercepting satellite communications (until May 2001 the FIS was not authorised to intercept foreign cable communications in Germany).

On the basis of differing legal provisions or the availability of a greater number of analysts, the capabilities of other intelligence services may be greater in detail terms in given areas. In particular, the monitoring of cable traffic increases the statistical likelihood of success, but not necessarily the number of communications which can be analysed. In fundamental terms, in your rapporteur's view the example of the FIS demonstrates the capabilities and strategies employed by foreign intelligence services in connection with the monitoring of foreign communications, even if those services do not disclose such matters to the public.

The FIS endeavours, by means of **strategic** telecommunications monitoring, to secure information from foreign countries about foreign countries. With that aim in view, satellite transmissions are intercepted using a series of search terms (which in Germany must be authorised in advance by the so-called G10 Committee[24]). The relevant figures break down as follows (year 2000): of the roughly 10 million international communications routed to and from Germany every day, some 800 000 are transmitted via satellite. Just under 10% of these (75 000) are filtered through a search engine. In your rapporteur's view, this limitation is not imposed by the law (in theoretical terms, and at least prior to the proceedings before the Federal Constitutional Court, a figure of 100% would have been allowable), but derives from technical restrictions, e.g. the limited capacity for analysis.

The number of usable search terms is likewise restricted on technical grounds and by the need to secure authorisation. The grounds for the judgment handed down by the Federal Constitutional Court refer, alongside the purely formal search terms (connections used by foreign nationals or foreign firms abroad), to 2 000 search terms in the sphere of nuclear proliferation, 1 000 in the sphere of the arms trade, 500 in the sphere of terrorism and 400 in the sphere of drug trafficking. However, the procedure has proved relatively unsuccessful in connection with terrorism and drug trafficking.

The search engine checks whether authorised search terms are used in fax and telex communications. Automatic word recognition in voice connections is not yet possible. If the search terms are not found, in technical terms the communications automatically end up in the waste bin; they cannot be analysed, owing to the lack of a legal basis. Every day, five or so communications are logged which are covered by the provisions governing the protection of the German constitution. The monitoring strategy of the FIS is geared to finding clues on which to base further monitoring activities. The monitoring of all foreign communications is not an objective. On the basis of the information available to your rapporteur, this also applies to the SIGINT activities of other foreign intelligence services.

[24] Law on the restriction of the privacy of posts and telecommunications (law on Article 10 of the Basic Law) of 13 August 1968.

4. Satellite communications technology

4.1. The significance of telecommunications satellites

Today, telecommunications satellites form an essential part of the global telecommunications network and have a vital role to play in the provision of television and radio programmes and multimedia services. Nevertheless, the proportion of international communications accounted for by satellite links has decreased substantially over the past few years in Central Europe; it lies between 0.4 and 5%[25]. This can be explained by the advantages offered by fibreoptic cables, which can carry a much greater volume of traffic at a higher connection quality.

Today, voice communications are also carried by digital systems. The capacity of digital connections routed via satellites is restricted to **1 890** ISDN-standard (64 kbits/sec) voice channels per transponder on the satellite in question. In contrast, **241 920** voice channels with the same standard can be carried on a single optical fibre. This corresponds to a ratio of **1:128**!

In addition, the quality of connections routed via satellite is lower than those routed via underwater fibreoptic cables. In the case of normal voice transmissions, the loss of quality resulting from the long delay times of several hundred milliseconds is hardly noticeable – although it is perceptible. In the case of data and fax connections, which involve a complicated 'handshaking' procedure, cable offers clear advantages in terms of connection security. At the same time, however, only 15% of the world's population is connected to the global cable network[26].

For certain applications, therefore, satellite systems will continue to offer advantages over cable in the long term. Here are some examples from the civilian sphere:

- National, regional and international telephone and data traffic in areas with a low volume of communications, i.e. in those places where the low rate of use would make a cable connection unprofitable;
- Temporary communications systems used in the context of rescue operations following natural disasters, major events, large-scale building sites, etc.;
- UN missions in regions with an underdeveloped communications infrastructure.
- Flexible/mobile business communications using very small earth stations (VSATs, see below).

This wide range of uses to which satellites are put in the communications sphere can be explained by the following characteristics: the footprint of a single geostationary satellite can cover almost 50% of the earth's surface; impassable regions no longer pose a barrier to communication. In the area concerned, 100% of users are covered, whether on land, at sea or in the air. Satellites can be made operational within a few months, irrespective of the infrastructure available on the spot, they are more reliable than cable and can be replaced more easily.

[25] Information drawn from the answers given to the Temporary Committee by telecommunications service providers from a number of Member States.
[26] Deutsche Telekom homepage: www.detesat.com/deutsch/

The following characteristics of satellite communications must be regarded as drawbacks: the relatively long delay times, the path attenuation, the shorter useful life, by comparison with cable, of 12 to 15 years, the greater vulnerability to damage and the ease of interception.

4.2. How a satellite link operates[27]

As already mentioned (see Chapter 3), by using appropriate antennae microwaves can be very effectively focused, allowing cables to be replaced by microwave radio links. If the transmitting and the receiving antenna are not in line of sight, but rather, as they are on the earth, on the surface of a sphere, then from a given distance onwards the receiving antenna 'disappears' below the horizon owing to the curvature of the earth. The two antennae are thus no longer in line of sight. This would apply, for example, to an intercontinental microwave radio link between Europe and the USA. The antennae would have to be fitted to masts 1.8 km high in order for a link to be established. For this reason, an intercontinental microwave radio link of this kind is simply not feasible, setting aside the issue of the attenuation of the signal by air and water vapour. However, if a kind of mirror for the microwave radio link can be set up in a 'fixed position' high above the earth in space, large distances can be overcome, despite the curvature of the earth, just as a person can see round corners using a traffic mirror. The principle described above is made workable through the use of geostationary satellites.

4.2.1. Geostationary satellites

If a satellite is placed into a circular orbit parallel to the equator in which it circles the earth once every 24 hours, it will follow the rotation of the earth exactly. Looking up from the earth's surface, it seems to stand still at a height of roughly 36 000 km – it has a **geostationary** position. Most communications and television satellites are satellites of this type.

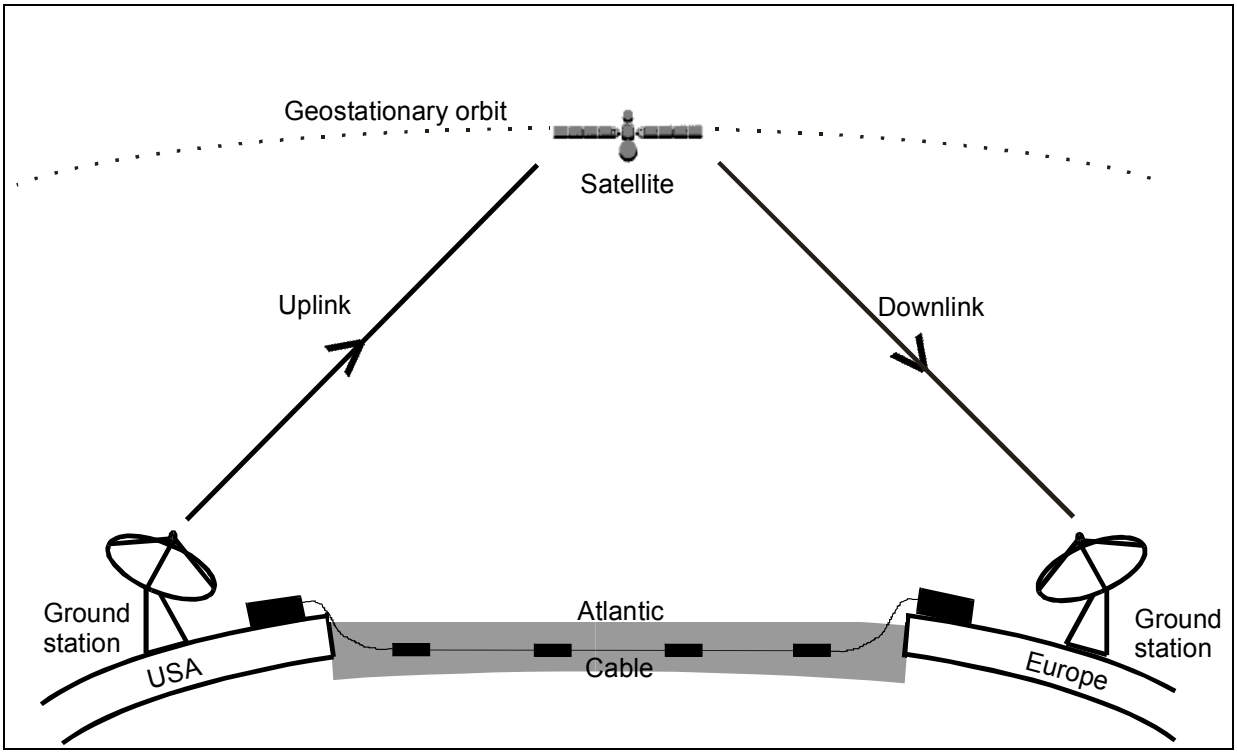
4.2.2. The route followed by signals sent via a satellite communication link

The transmission of signals via satellite can be described as follows:

The signal coming from a cable is transmitted by an earth station equipped with a parabolic antenna to the satellite via an upward microwave radio link, the **uplink**. The satellite receives the signal, regenerates it and transmits it back to another Earth station via a downwards microwave radio link, the **downlink**. From there, the signal is transferred back to a cable network.

In the case of mobile communications satellite telephones the signal is transmitted directly from the mobile communications unit to the satellite, from where it can be fed into a cable link, via an Earth station, or directly transmitted to a different mobile unit.

[27] *Hans Dodel*, Satellite communications, Hüthig Verlag (1999), *Georg E. Thaller*, Satellites in Earth Orbit, Franzisverlag (1999)



4.2.3. The most important satellite communication systems

If necessary, communications coming from **public cable networks** (not necessarily state networks) are transmitted between fixed earth stations, via satellite systems of differing scope, and then fed back into cable networks. A distinction is drawn between the following forms of satellite systems:

- global systems (e.g. INTELSAT)
- regional (continental) systems (e.g. EUTELSAT)
- national systems (e.g. ITALSAT).

Most of these satellites are in a geostationary orbit; 120 private companies throughout the world operate some 1 000 satellites[28].

In addition, the far northern areas of the earth are covered by satellites in a highly elliptical orbit (Russian molnyia orbits) in which the satellites are visible to users in the far north for half their orbit. In principle, two satellites can provide full regional coverage[29], which is not feasible from a geostationary position above the equator. In the case of the Russian Molnyia satellites, which have been in service as communications satellites since 1974 (prototype launched in 1964), three equidistant satellites orbit the earth once every 12 hours and thus guarantee continuous transmission of communications[30].

[28] *Georg E. Thaller*, Satellites in Earth Orbit, Franzisverlag (1999).
[29] Cf. *Hans Dodel*, Satellite communications, Hüthig Verlag (1999)
[30] Hompage of the Federation of American Scientists, http://www.geo-orbit.org

Alongside this, the global INMARSAT system – originally established for use at sea – provides a **mobile communications system** by means of which satellite links can be established anywhere in the world. This system also uses geostationary satellites.

The worldwide satellite-based mobile telephone system IRIDIUM, which employed a number of satellites placed at time intervals in low orbits, recently ceased operating on economic grounds (overcapacity).

There is also a rapidly expanding market for so-called VSAT links (VSAT = very small aperture terminal). This involves the use of very small earth stations with antennae with a diameter of between 0.9 and 3.7 metres, which are operated either by firms to meet their own needs (e.g. videoconferences) or by mobile service providers to meet short-term communications requirements (e.g. in connection with meetings). In 1996, 200 000 very small earth stations were in operation around the world. Volkswagen AG operates 3 000 VSAT units, Renault 4 000, General Motors 100 000 and the largest European oil company 12 000. If the client does not arrange for encryption, communication is entirely open[31].

4.2.3.1. Global satellite systems

Through the positioning of satellites above the Atlantic, Indian and Pacific regions, these satellite systems cover the entire globe.

INTELSAT[32]

INTELSAT (International Telecommunications Satellite Organisation) was founded as an authority in 1964 with an organisational structure similar to that of the UN and with the commercial purpose of providing international communications. The members of the organisation were state-owned telecommunications companies. Today, 144 governments are INTELSAT members. In 2001, INTELSAT will be privatised.

INTELSAT now operates a fleet of 20 geostationary satellites, which provide links between more than 200 countries and whose services are rented out to the members of INTELSAT. The members operate their own ground stations. Following the establishment of INTELSAT Business Service (IBS) in 1984, non-members (e.g. telephone companies, large firms, international concerns) can also use the satellites. INTELSAT offers global services such as communications, television, etc. Telecommunications are transmitted via the C-band and the Ku-band (see below).

INTELSAT satellites are the most important international telecommunications satellites, accounting for a very large proportion of the world market in such communications.

The satellites cover the Atlantic, Indian and Pacific regions (see table, Chapter 5.3).

Ten satellites are positioned above the Atlantic between 304°E and 359°E, the Indian region is covered by six satellites situated between 62°E and 110m.5°E and the Pacific region by three

[31] *Hans Dodel*, private information.
[32] INTELSAT homepage: http://www.intelsat.com

satellites situated between 174°E and 180°E. The high volume of traffic in the Atlantic region is covered by a number of individual satellites positioned at the relevant longitudes.

INTERSPUTNIK[33]

In 1971 the international communications organisation INTERSPUTNIK was founded by nine countries as an agency of the former Soviet Union with a task similar to that of INTELSAT. Today, INTERSPUTNIK is an international organisation which the government of any country can join. It now has 24 member countries (including Germany) and some 40 users (including France and the UK), which are represented by their post offices or national telecommunications companies. Its headquarters are in Moscow.

Telecommunications are transmitted via the C-band and the Ku-band (see below).

Its satellites (Gorizont, Express and Express A, owned by the Russian Federation, and LMI-1, the product of the Lockheed-Martin joint venture) also cover the entire globe: one satellite is positioned above the Atlantic region, with a second planned, three are positioned above the Indian region and two are positioned above the Pacific region (see table, Chapter 5.3).

INMARSAT[34]

Since 1979 INMARSAT (Interim International Maritime Satellite) has provided, by means of its satellite system, worldwide **mobile** communications at sea, in the air and on land and an emergency radio system. INMARSAT was set up as an international organisation at the instigation of the International Maritime Organisation. INMARSAT has since been privatised and has its headquarters in London.

The INMARSAT system consists of nine satellites in geostationary orbits. Four of these satellites – the INMARSAT-III generation – cover the entire globe with the exception of the high polar areas. Each individual satellite covers roughly one-third of the earth's surface. Through their positioning above the four ocean regions (West and East Atlantic, Pacific, Indian Ocean), global coverage is provided. At the same time, each INMARSAT has a number of spot beams which make it possible to focus energy in areas with heavier communications traffic.

Telecommunications are transmitted via the L-band and the Ku-band (see below; 4.2.4).

PANAMSAT[35]

PanAmSat was founded in 1988 as a commercial provider of a global satellite system and has its headquarters in the USA. PanAmSat now has a fleet of 21 satellites which provide services such as television, Internet and telecommunications on a worldwide basis, albeit chiefly in the USA.

Telecommunications are transmitted via the C-band and the Ku-band. Of the 21 satellites, seven cover the Atlantic region, two the Pacific region and two the Indian Ocean region. The footprints

[33] INTERSPUTNIK homepage: http://www.intersputnik.com
[34] INMARSAT homepage: http://www.inmarsat.com
[35] PANAMSAT homepage: http://www.panamsat.com

of the remaining satellites cover North and South America. The PanAmSat satellites play only a secondary role in communications in Europe.

4.2.3.2. Regional satellite systems

Individual regions/continents are covered by the footprints of regional satellite systems. As a result, the communications transmitted via them can be received only in those regions.

EUTELSAT[36]

EUTELSAT was founded in 1977 by 17 European postal administrations with the aim of meeting Europe's specific satellite communication requirements and supporting the European space industry. It has its headquarters in Paris and some 40 member countries. EUTELSAT is to be privatised in 2001.

EUTELSAT operates 18 geostationary satellites which cover Europe, Africa and large parts of Asia and establish a link with America. The satellites are positioned between 12.5°W and 48°E. EUTELSAT mainly offers television (850 digital and analog channels) and radio (520 channels) services, but also provides communication links – primarily within Europe, including Russia, e.g. for videoconferences, for the private networks run by large undertakings (including General Motors and Fiat), for press agencies (Reuters, AFP), for providers of financial information and for mobile data transmission services.

Telecommunications are transmitted via the Ku-band.

ARABSAT[37]

ARABSAT is the counterpart to EUTELSAT in the Arab region and was founded in 1976. Membership is made up of 21 Arab countries. ARABSAT satellites are used both for the transmission of television services and for communications.

Telecommunications are transmitted mainly via the C-band.

PALAPA[38]

The Indonesian PALAPA system has been in operation since 1995 and is the south-Asian counterpart to EUTELSAT. Its footprint covers Malaysia, China, Japan, India, Pakistan and other countries in the region.

Telecommunications are transmitted via the C-band and the Ku-band.

[36] EUTELSAT homepage: http://www.eutelsat.com
[37] ARABSAT homepage: http://www.arabsat.com
[38] *Hans Dodel*, Satellite communications, Hüthigverlag (1999)

4.2.3.3. National satellite systems[39]

Many states meet their own requirements by operating satellite systems with restricted footprints.

One purpose of the French telecommunications satellite **TELECOM** is to link the French departments in Africa and South America with mainland France. Telecommunications are transmitted via the C-band and the Ku-band.

ITALSAT operates telecommunications satellites which cover the whole of Italy by means of a series of restricted footprints. Reception is therefore possible only in Italy. Telecommunications are transmitted via the Ku-band.

AMOS is an Israeli satellite whose footprint covers the Middle East. Telecommunications are transmitted via the Ku-band.

The Spanish **HISPASAT** satellites cover Spain and Portugal (KU-spots) and transmit Spanish television programmes to North and South America.

4.2.4. The allocation of frequencies

The International Telecommunications Union (ITU) is responsible for the allocation of frequencies. For ease of organisation, for radio communication purposes the world has been divided into three regions:

1. Europe, Africa, former Soviet Union, Mongolia
2. North and South America and Greenland
3. Asia, with the exception of countries in region 1, Australia and the South Pacific.

This division, which has become established over the years, was taken over for the purposes of satellite communications and has led to the positioning of large numbers of satellites in certain geostationary areas. The most important frequency bands for satellite communications are:

- the L-band (0.4 – 1.6 GHz) for mobile satellite communications, e.g. via IMMARSAT;
- the C-band (3.6 – 6.6 GHz) for earth stations, e.g. via INTELSAT;
- the Ku-band (10 – 20 GHz) for earth stations, e.g. INTELSAT Ku-spot and EUTELSAT;
- the Ka-band (20 – 46 GHz) for earth stations, e.g. military communications satellites (see Chapter 4.4.3);
- the V-band (46 – 56 GHz) for very small earth stations (VSATs).

4.2.5. Satellite footprints

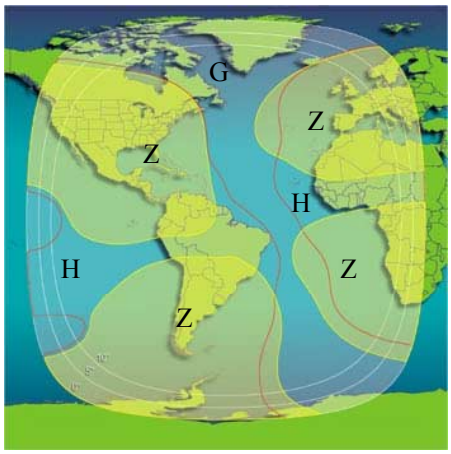
The footprint is the area on the earth covered by a satellite antenna. It may embrace up to 50% of the earth's surface, or, by means of signal focusing, be restricted to small, regional spots.

The higher the frequency of the signal emitted, the more it can be focused and the smaller the footprint becomes. The focusing of the satellite signal on smaller footprints can increase the

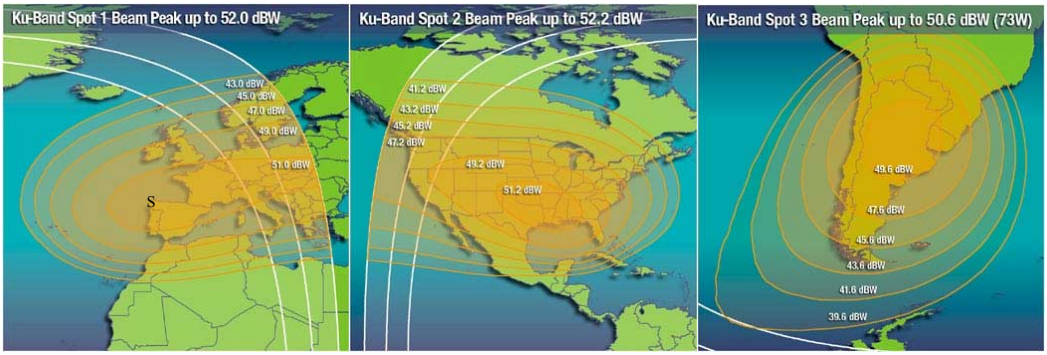
[39] *Hans Dodel* and Internet research

energy of the signal. The smaller the footprint, the stronger the signal, and thus the smaller the receiving antennae may be.

This can briefly be illustrated in greater detail, taking the example of the INTELSAT satellites[40].



The footprints of the INTELSAT satellites are divided into various beams:
Each satellite's global beam (G) covers roughly one-third of the earth's surface; the hemispheric beams (H) each cover an area slightly smaller than half that covered by the global beams. Zone beams (Z) are spots in particular areas of the earth; they are smaller than the hemi-beams. In addition there are so-called spot beams; these are small, precise footprints (see below).



The global, hemispheric and zone beams use C-band frequencies. The spot beams use Ku-band frequencies.

4.2.6. The size of antennae required by an earth station

Parabolic antennae with a diameter of between 0.5 and 30m are used as receiving antennae on the earth. The parabolic mirror reflects all incoming waves and focuses them. The actual receiving system is situated in the focal point of the parabolic mirror. The greater the energy of the signal at the receiving point is, the smaller the diameter of the parabolic antenna need be.

[40] INTELSAT satellite 706, 307°E, footprints taken from the INTELSAT homepage, http://www.intelsat.com

The key factor in connection with the investigations conducted for this report is that a proportion of intercontinental communications are transmitted via the C-band in the global beams of the INTELSAT satellites and other satellites (e.g. INTERSPUTNIK) and that satellite antennae with a diameter of roughly 30 m are needed to receive some of these communications (see Chapter 5). Antennae of that size were also needed for the first stations set up to intercept satellite communications, since the first generation of INTELSAT satellites had only global beams and signal transmission technology was much less sophisticated than it is today. These antennae, some of which have a diameter of more than 30 m, are still used at the stations in question, even though they are no longer required on purely technical grounds (see also Chapter 5, 5.2.3.).

Today, the typical antennae required for INTELSAT communications in the C-band have a diameter of between 13 and 20 m.

Antennae with a diameter of between 2 and 5 m are required for the Ku-spots of the INTELSAT satellites and other satellites (EUTELSAT Ku-band, AMOS Ku-band, etc.).

In the case of very small earth stations, which operate in the V-band and whose signal, by virtue of the high frequency, can be focused even more strongly than those in the Ku-band, antennae with a diameter of between 0.5 and 3.7 m are adequate (e.g. VSATs from EUTELSAT or INMARSAT).

4.3. Satellite communications for military purposes

4.3.1. General

Communications satellites play an important role in the military sphere as well. Many countries, including the USA, the United Kingdom, France and Russia, operate their own geostationary military communications satellites, with the aid of which independent global communication is possible The USA has stationed one satellite roughly every 10° around the earth in some 32 orbital positions. However, some use is also made of commercial geostationary satellites for the purposes of providing military communications.

4.3.2 Frequencies used for military purposes

The frequency bands used for military communications lie in the range between 4 Ghz and 81 Ghz. The bands typically used by military communications satellites are X-band (SHF - 3-30 Ghz) and the Ka-band (EHF - 20-46 Ghz).

4.3.3. Size of the receiving stations

A distinction must be drawn between mobile stations, which may have a diameter of only a few decimetres, and fixed stations, which generally have a diameter not exceeding 11m. There are, however, two types of antenna (to receive signals from DSCS satellites) with a diameter of 18m.

4.3.4. Examples of military communications satellites

The US **MILSTAR** program (Military Strategy, Tactical and Relay Satellite System), which operates six geostationary satellites worldwide, enables US armed forces to communicate with

each other and with command centres using small earth stations, aircraft, ships and man-packs. Through the link among the satellites themselves worldwide communications availability is guaranteed even if all the US earth stations cease operating.

The **DSCS** (Defense Satellite Communications System) also provides global communications by means of five geostationary satellites. The system is used by the US armed forces and some government agencies.

The British military satellite system **SKYNET** also provides global communications.

The French system **SYRACUSE**, the Italian system **SICRAL** and the Spanish system fly piggy-back on their respective national civilian communications satellites and provide military communications, albeit only on a regional basis, in the S-band.

The Russians guarantee their armed forces' communications by means of transponders in the X-band used by the Molnyia satellites.

NATO operates its own communications satellites (**NATO IIID, IVA** and **IVB)**. The satellites provide voice, telex and data links between military units.

5. Clues to the existence of at least one global interception system

5.1. Why is it necessary to work on the basis of clues?

It is only natural that secret services do not disclose details of their work. Consequently there is, at least officially, no statement by the foreign intelligence services of the UKUSA states that they work together to operate a global interception system. The existence of such a system thus needs to be proved by gathering as many clues as possible, thereby building up a convincing body of evidence.

The trail of clues which constitutes evidence of this kind is made up of three elements:

- evidence that the foreign intelligence services in the UKUSA states intercept private and business communications;
- evidence that interception stations operated by the UKUSA states are to be found in the parts of the world where they would be needed in the light of the technical requirements of the civilian satellite communication system;
- evidence that there is a closer than usual association between the intelligence services of these states. For the purposes of proving the existence of such an association, it is irrelevant whether this extends to the acceptance from partners of applications for the interception of messages which are then forwarded to them in the form of unevaluated raw material. This question is only relevant when investigating the hierarchies within such an interception association.

5.1.1. Evidence of interception activity on the part of foreign intelligence services

At least in democracies, intelligence services work on the basis of laws which define their purpose and/or powers. It is thus easy to prove that in many of these countries foreign intelligence services exist which intercept civilian communications. This is true of the five UKUSA states, which all operate such services. There is no need for specific additional proof that any of these states intercept communications entering and leaving their territory. Satellite communications also permit some intelligence communications intended for recipients abroad to be intercepted from the country's own territory. In none of the five UKUSA states is there any legal impediment to intelligence services doing this. The logic underlying the method for the strategic monitoring of foreign communications, and its at least partly overtly acknowledged purpose, make it practically certain that the intelligence services do in fact use it to that end.[41]

5.1.2. Evidence for the existence of stations in the necessary geographical areas

The only restriction on the attempt to build up worldwide monitoring of satellite communications arises from the technical constraints imposed by these communications themselves. There is no place from which **all** satellite communications can be intercepted (see Chapter 4, 4.2.5.).

It would be possible for a worldwide interception system to be constructed, subject to three conditions:

[41] Your rapporteur has evidence that this is the case. Source protected.

- the operator has national territory of its own in all the necessary parts of the world;
- the operator has, in all the necessary parts of the world, either national territory of its own or a right of access entitling it to operate or share the use of stations;
- the operator is a group of states which has formed an intelligence association and operates the system in the necessary parts of the world.

None of the UKUSA states would be able to operate a global system on its own. The USA has, at least formally, no colonies. Canada, Australia and New Zealand also have no territory outside the narrower confines of their countries, and the UK would also not be able to operate a global interception system on its own.

5.1.3. Evidence of a close intelligence association

On the other hand it has not been disclosed whether and to what extent the UKUSA states cooperate with one another in the intelligence field. Normally cooperation between intelligence services takes place bilaterally and on the basis of an exchange of evaluated material. A multilateral alliance is in itself something very unusual; if one adds to this the regular exchange of raw material, this would be a qualitatively new form of cooperation. The existence of such an association can only be proved on the basis of clues.

5.2. How can a satellite communications interception station be recognised?

5.2.1. Criterion 1: Accessibility of the installation

Installations with large antennae belonging to the post office, broadcasting organisations or research institutions are accessible to visitors, at least by appointment; interception stations are not. They are generally operated, at least in name, by the military, which also carries out at least part of the technical work of interception. In the case of the stations run by the USA, for example, operations are carried out jointly with the NSA by the Naval Security Group (NAVSECGRU), the United States Army Intelligence and Security Command (INSCOM) or the Air Intelligence Agency (AIA). In the British stations, the British intelligence service GCHQ operates the installations jointly with the Royal Air Force (RAF). This arrangement enables the installations to be guarded with military efficiency and at the same time serves as cover.

5.2.2. Criterion 2: Type of antenna

Various types of antennae are used in the installations which fulfil criterion 1, each with a different characteristic shape, which provides evidence as to the purpose of the interception station. Arrangements of tall rod antennae in a large-diameter circle (Wullenweber antennae), for example, are used for locating the direction of radio signals. Similarly, circular arrangements of rhombic-shaped antennae (Pusher antennae) serve the same purpose. Omnidirectional antennae, which look like giant conventional TV antennae, are used to intercept non-directional radio signals. **To receive satellite signals, however, only parabolic antennae are used.** If the parabolic antennae are standing on an open site, it is possible to calculate on the basis of their position, their elevation and their compass (azimuth) angle which satellite is being received. This is possible, for example, in Morwenstow (UK), Yakima (USA) or Sugar Grove (USA).

However, most often parabolic antennae are concealed under spherical white covers known as radomes: these protect the antennae, but also conceal which direction they are pointing in.

If parabolic antennae or radomes are positioned on an interception station site, one may be certain that they are receiving signals from satellites, though this does not prove what type of signals these are.

5.2.3. Criterion 3: Size of antenna

Satellite receiving antennae on a site which meets criterion 1 may be intended for various purposes:
- receiving station for military communications satellites;
- receiving station for spy satellites (pictures, radar);
- receiving station for SIGINT satellites;
- receiving station for interception of civilian communications satellites.

It is not possible to tell from outside what function these antennae or radomes serve. However, the diameter of the antennae gives some clues as to their purpose. There are minimum sizes, dictated by technical requirements, for antennae intended to receive the 'global beam' in the C-band of satellite-based civilian international communications. The first generation of these satellites needed antennae with a diameter of 25-30 m; nowadays 15-20 m is enough. The automatic computer filtering of signals received calls for the highest possible signal quality, so for intelligence purposes an antenna at the upper end of the scale is chosen.

In the sphere of military communications as well, command centres have two types of antenna with a diameter of roughly 18 m (AN/FSC-78 and AN/FSC-79). However, most antennae for military communications have a much smaller diameter, since they must be transportable (tactical stations).

In view of the nature of the signals transmitted back to the station (high degree of focusing and high frequency), earth stations for SIGINT satellites need only small antennae. This also applies to antennae which receive signals from spy satellites.

If a site houses two or more satellite antennae with a diameter of at least 18 m, one of its tasks is certainly that of intercepting civilian communications. In the case of a station housing US forces, one of the antennae may also be used to receive military communications.

5.2.4. Criterion 4: Evidence from official sources

Official descriptions of the tasks of some stations have been published. In that connection governments and military units are regarded as official sources. If this criterion has been met, the others become superfluous.

5.3. Publicly accessible data about known interception stations

5.3.1. Method

With a view to determining which stations meet the criteria set out in Chapter 5.2. and thus form part of the global interception system and establishing what tasks they have, the relevant, somewhat contradictory, literature (Hager[42], Richelson[43], Campbell[44]) declassified documents[45], the homepage of the Federation of American Scientists[46] and operators' homepages[47] (NSA, AIA, etc.) and other Internet publications were analysed. In the case of the New Zealand station in Waihopai, the New Zealand Government has drawn up an official description of its tasks[48]. In addition, the footprints of telecommunications satellites were collated, the requisite antenna sizes were calculated and these footprints and antenna locations were entered, along with the locations of possible stations, on world maps.

5.3.2. Detailed analysis

The following principles relating to the physics of satellite communications apply in connection with the analysis (see also Chapter 4):

- A satellite antenna can only record communications transmitted within the footprint in which it is located. In order to receive communications, which are mainly transmitted in the C-band and Ku-band, an antenna must lie within the footprints containing those bands.
- A satellite antenna is required for each separate global beam, even if beams from two satellites overlap.
- If a satellite has other footprints in addition to the global beam, which is typical of today's generations of satellites, a single satellite antenna can no longer record all the communications transmitted via that satellite, since a single satellite antenna cannot be located in every one of the satellite's footprints. In order to capture a satellite's hemispheric beam and its global beam, therefore, two satellite antennae are required in different areas (see illustration of the footprints in Chapter 4). If further beams (zone and spot beams) are involved, further satellite antennae are required. In principle, different, overlapping beams

[42] *Nicky Hager*: Exposing the Global Surveillance System http://www.ncoic.com/echelon1.htm
Nicky Hager: Secret Power. New Zealand's Role in the International Spy Network, Craig Potton Publishing (1996).
[43] *Jeffrey T. Richelson*, Desperately Seeking Signals, The Bulletin of the Atomic Scientists, Vol 56, No. 2, 47-51, http://www.bullatomsci.org/issues/2000/ma00/ma00richelson.html
Richelson, T. Jeffrey, The U.S. Intelligence Community, Westview Press (1999).
[44] *Duncan Campbell*, The state of the art in Communications Intelligence (COMINT) of automated processing for intelligence purposes of intercepted broadband multi-language leased or common carrier systems, and its applicability to COMINT targeting and selection, including speech recognition, Part 4/5, in STOA (Ed.). Development of Surveillance Technology and Risk of Abuse of Economic Information, (October 1999), PE 168.184 http://www.europarl.eu.int/dg4/stoa/en/publi/pdf/98-14-01-2en.pdf
Duncan Campbell: Inside Echelon, 25.7.2000, http://www.heise.de/tp/deutsch/special/ech/6928/1.html
Campbell, Duncan: Interception Capabilities Impact and Exploitation – Echelon and its role in COMINT, submitted to the Temporary Committee on 22 January 2001
Federation of American Scientists, http://www.fas.org/irp/nsa/nsafacil.html
[45] *Jeffrey T. Richelson*: Newly released documents on the restrictions NSA places on reporting the identities of US persons: Declassified: http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB23/index.html
[46] Federation of American Scientists (FAS), http://www.fas.org/irp/nsa/nsafacil.html.
[47] Military.com; *.mil-Homepages.
[48] Domestic and External Security Secretariat, Department of the Prime Minister and Cabinet, Securing our Nation's Safety (2000), http://www.dpmc.govt.nz/dess/securingoursafety/index.html

from a single satellite can be captured by one satellite antenna, since it is technically feasible to separate different frequency bands when reception takes place, although this leads to a deterioration in the signal-noise ratio.

In addition, the requirements referred to in Chapter 5.2. apply: the non-accessibility of the installations, on the grounds that they are operated by the military[49], the fact that parabolic antennae are required to receive satellite signals and the fact that the size of the satellite antennae needed to capture the C-band in the global beam at least 30 m for the first INTELSAT generation and more than 15 to 18 m for later generations. The official descriptions of the tasks of some of the stations have been cited as evidence of their role in interception operations.

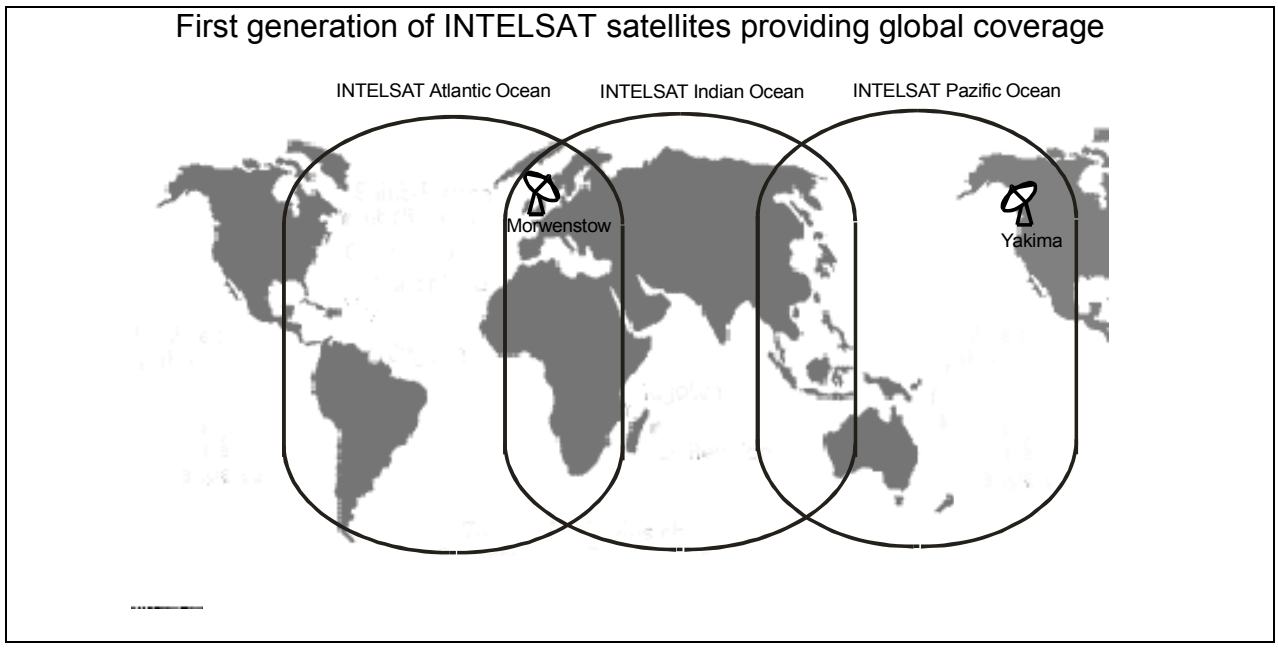
5.3.2.1. The parallel between the development of INTELSAT and the building of stations

A global interception system must grow as communications develop. Accordingly, the start of the satellite communications era must lead to the establishment of stations and the introduction of new generations of satellites must lead to the establishment of new stations and the building of new satellite antennae which can cope with the new technical requirements. The number of stations and the number of satellite antennae must increase whenever this is necessary in order to cover the full volume of communications traffic.
If we turn this equation round, it is no coincidence that, when new footprints come into being, new stations are established and new satellite antennae are built. Instead, this can be seen as a clue to the existence of a communications interception station.
Since the INTELSAT satellites were the first telecommunications satellites, and, moreover, the first to cover the entire globe, it is only logical that the introduction of the new generations of INTELSAT satellites should go hand-in-hand with the establishment of new and bigger stations.

The first global generation

As long ago as 1965 the first INTELSAT satellite (Early Bird) was placed in a geostationary orbit. Its transmission capacity was still low and its footprint covered only the northern hemisphere.
When the second and third INTELSAT generations came into operation, in 1967 and 1968 respectively, global coverage was achieved for the first time. The satellites' global beams covered the Atlantic, Pacific and Indian Ocean areas. Satellite systems with smaller footprints had not yet been introduced. Three satellite antennae were thus needed in order to record all communications. Since two of the global beams overlapped over the European continent, in that area the global footprints of two satellites could be covered by two satellite antennae trained in different directions.

[49] Abbreviations used: NAVSECGRU: Naval Security Group, INSCOM: United States Army Intelligence And Security Command, AIA: Air Intelligence Agency, IG: Intelligence Group, IS: Intelligence Squadron, IW: Intelligence Wing, IOG: Information Operation Group, MIG: Military Intelligence Group.

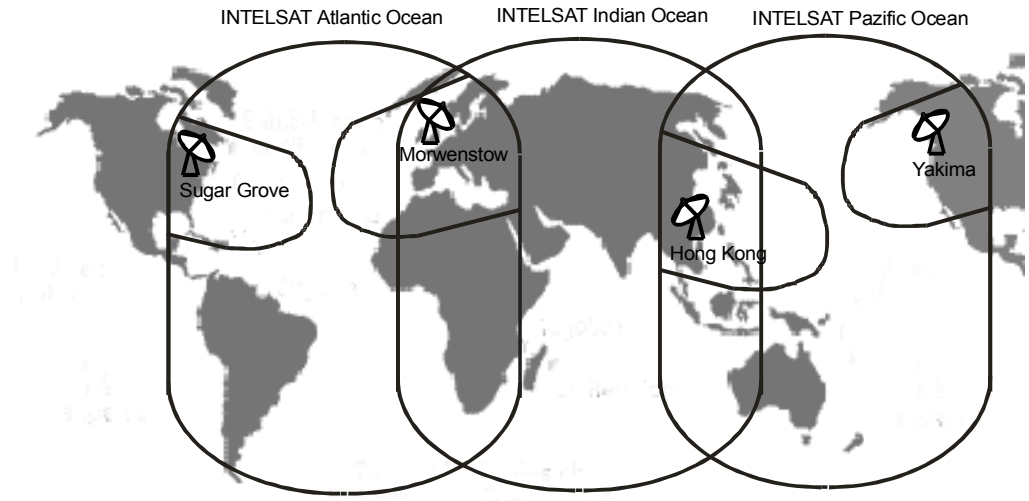


In the early 1970s the **Yakima** station was established in the north-western USA and in 1972/73 the **Morwenstow** station was built in southern England. At that time, Yakima had one large antenna (trained towards the Pacific) and Morwenstow had two large antennae (one trained towards the Atlantic, the other towards the Indian Ocean). By virtue of the location of the two stations, all communications could be recorded.

The second global generation

The second generation of INTELSAT satellites (IV and IVA) were developed in the 1970s and placed in a geostationary orbit (1971 and 1975). The new satellites, which also provided global coverage and had a much larger number of communications channels (4000-6000), used, in addition to the global beams, zone beams in the northern hemisphere (see Chapter 4). One zone beam covered the eastern USA, a second the western USA, a third western Europe and a fourth east Asia. As a result, it was no longer possible to record all communications using two stations equipped with three satellite antennae. Using the existing stations in Yakima, the zone beam in the western USA could be covered; Morwenstow covered the zone beam over Europe. A station in the eastern USA and another in east Asia were needed in order to cover the other two zone beams.

Second generation of INTELSAT satellites providing global coverage



In the late 1970s the **Sugar Grove** station in the eastern USA was developed (the station already existed for the purpose of intercepting Russian communications); it came into operation in 1980. A station in **Hong Kong** was also set up in the late 1970s.
As a result, in the 1980s global interception of INTELSAT communications was possible using the four stations - Yakima, Morwenstow, Sugar Grove and Hong Kong.

The later INTELSAT satellites, which used zone beams and spot beams in addition to the global and hemispheric beams, made further stations in various parts of the world necessary. Here, on the basis of the information available, it is difficult to document a link with the development of further stations and/or the introduction of new satellite antennae.

Since it is equally difficult to gain access to information about stations, it cannot be determined with any certainty which satellites using which beams are covered by which stations. However, the footprints in which known stations are located can be determined.

5.3.2.2. Global coverage by means of stations which are known to intercept transmissions from telecommunications satellites

Today, global satellite communications are provided by satellites operated by INTELSAT, INMARSAT and INTERSPUTNIK. The division of the earth into three footprints (Indian Ocean, Pacific and Atlantic areas), introduced when the first generations of satellites were sent into space, has been retained. In each of the footprints there are stations which meet the criteria which characterise them as interception stations:

Satellites over the Indian Ocean:

INTELSAT 604 (60°E), 602 (62°E), 804 (64°E), 704 (66°E) EXPRESS 6A (80°E) INMARSAT Indian Ocean area	Geraldton, Australia Pine Gap, Australia Morwenstow, England Menwith Hill, England
INTELSAT APR1 (83°), APR-2 (110,5°)	Geraldton, Australia Pine Gap, Australia Misawa, Japan

Satellites over the Pacific:

INTELSAT 802 (174°), 702 (176°), 701 (180°) GORIZONT 41 (130°E), 42 (142°E), LM-1 (75°E) INMARSAT Pacific area	Waihopai, New Zealand Geraldton, Australia Pine Gap, Australia Misawa, Japan Yakima, USA - only Intelsat and Inmarsat

Satellites over the Atlantic:

INTELSAT 805 (304,5°), 706 (307°), 709 (310°) 601 (325,5°), 801 (328°), 511(330,5°), 605 (332,5°), 603 (335,5°), 705 (342°) EXPRESS 2 (14°W), 3A (11°W) INMARSAT Atlantic area	Sugar Grove, USA Sabana Seca, Puerto Rico Morwenstow, England Menwith Hill, England
INTELSAT 707 (359°)	Morwenstow, England Menwith Hill, England

This shows that the global interception of communications is feasible.

In addition, there are further stations which, although they do not meet the criterion of antenna size, and although there is no other clear evidence underpinning the assumption, may still form part of the global interception system. These stations could be used to cover the zone or spot beams of satellites whose global beams are intercepted by other stations or for whose global beam no large satellite antennae are required.

5.3.2.3. The stations in detail

In the detailed descriptions of the stations a distinction is drawn between stations which are clearly used to intercept transmissions from telecommunications satellites (criteria outlined in Chapter 5, 5.2.) and stations whose role cannot definitely be proven with the aid of those criteria.

5.3.2.3.1. Stations used to intercept transmissions from telecommunications satellites

The following stations meet the criteria outlined in Chapter 5.2., criteria which point to a role in intercepting transmissions from telecommunications satellites:

Yakima, USA (120°W, 46°N)
The station was established in the 1970s, at the same time as the first generation of satellites were put into orbit. Since 1995, the Air Intelligence Agency (AIA), 544th Intelligence Group (Detachment 4), has been stationed in Yakima, along with the Naval Security Group (NAVSECGRU). Six satellite antennae have been installed on the site; the sources give no clue as to the size of the antennae. Hager describes the antennae as large and claims that they are trained on INTELSAT satellites over the Pacific (two satellite antennae) and INTELSAT satellites over the Atlantic, and on INMARSAT Satellite 2.
The fact that Yakima was established at the same time as the first generation of INTELSAT satellites went into orbit, and the general description of the tasks of the 544th Intelligence Group, suggest that the station has a role in global communications surveillance. A further clue is provided by Yakima's proximity to a normal satellite receiving station, which lies 100 miles to the north.

Sugar Grove, USA (80°W, 39°N)
Sugar Grove was established at the same time as the second generation of INTELSAT satellites came into operation, in the late 1970s. The NAVSECGRU and the AIA, 544th Intelligence Group (Detachment 3), are stationed at Sugar Grove. According to information provided by a variety of authors, the station has 10 satellite antennae, three of which have a diameter greater than 18 m (18.2 m, 32.3 m and 46 m) and which are thus clearly used to intercept transmissions from telecommunications satellites. One of the tasks performed at the station by Detachment 3 of the 544th IG is to provide intelligence support for the collection by Navy field stations of information transmitted by telecommunications satellites[50].
In addition, Sugar Grove is situated close (60 miles) to the normal satellite receiving station in Etam.

Sabana Seca, Puerto Rico (66°W, 18°N)
NAVSECGRU was first stationed in Sabana Seca in 1952. In 1995, it was joined by the AIA, 544th IG (Detachment 2). The station has at least one satellite antenna with a diameter of 32 m and four further small satellite antennae.
According to official information, the station's tasks are to perform 'satellite communication processing', to provide 'cryptologic and communications service' and to support Navy and DoD operations, including the collection of COMSAT information (from a description of the 544th IG). In future, Sabana Seca is set to become the first field station for the analysis and processing of satellite communications.

Morwenstow, England (4°W, 51°N)
Like Yakima, Morwenstow was established in the early 1970s, at the same time as the first generation of INTELSAT satellites went into space. Morwenstow is operated by the British Intelligence Service (GCHQ). The Morwenstow site houses some 21 satellite antennae, three of which have a diameter of 30 m; no details are available of the size of the other antennae.
No official information has been issued regarding the station's role; however, the size and number of the satellite antennae and the location of the station, only 110 km from the telecommunications station in Goonhilly, leave no doubt as to its task of intercepting transmissions from telecommunications satellites.

[50] 'It provides enhanced intelligence support to Air Force operational commanders and other consumers of communications satellite information collected by Navy-commanded field stations', from the home page of the 544th Intelligence Group http://www.aia.af.mil

Menwith Hill, England (2°W, 53°N)
Menwith Hill was established in 1956 and by 1974 already housed eight satellite antennae. Today, the figure is roughly 30, some 12 of which have a diameter of more than 20 m. At least one of the large antennae, although certainly not all, is a receiving antenna for military communications (AN/FSC-78). The British and Americans work together at Menwith Hill. The US services stationed there are NAVSECGRU, the AIA (451st IOS) and INSCOM, which has command of the station. The land on which Menwith Hill stands belongs to the UK Defence Ministry and is rented to the US Administration. According to official information, Menwith Hill's role is 'to provide rapid radio relay and to conduct communications research'. According to statement by Richelson and the Federation of American Scientists, Menwith Hill is both an earth station for spy satellites and an interception station for transmissions from Russian telecommunications satellites.

Geraldton, Australia (114°O, 28°S)
The station was established in the early 1990s. It is run by the Australian Secret Service (DSD), and it is partly manned by British servicemen previously stationed in Hong Kong (see above). According to Hager, four satellite antennae, of the same size (diameter of roughly 20 m) are trained on satellites above the Indian Ocean and the Pacific.
According to statements made under oath in the Australian Parliament by an expert, transmissions from civilian telecommunications satellites are intercepted at Geraldton[51].

Pine Gap, Australia (133°O, 23°S)
The station in Pine Gap was established in 1966. It is run by the Australian Secret Service (DSD), and roughly half of the 900 station personnel are Americans from the CIA and NAVSECGRU[52].
Pine Gap has 18 satellite antennae, one with a diameter of roughly 30 m and another with a diameter of roughly 20 m. According to official sources, and information provided by various authors, since its inception Pine Gap has been an earth station for SIGINT satellites. Station personnel control and guide various spy satellites and receive, process and analyse their signals. The large satellite antennae also suggest that transmissions from telecommunications satellites are intercepted, since no such antennae are required for work with SIGINT satellites. Until 1980 no Australians were allowed to work in the signals analysis department; since then, they have been granted free access to all parts of the station, with the exception of the Americans' own cryptography room.

Misawa, Japan (141°O, 40°N)
The station in Misawa was established in 1948 as the site for an HFDF antenna. It is manned by Japanese and Americans. The US services represented are NAVSECGRU, INSCOM and some AIA groups (544th IG, 301st IS). The site houses around 14 satellite antennae, some of which have a diameter of roughly 20 m (estimate). Officially, Misawa acts as a 'cryptology operations centre'. According to information supplied by Richelson, the station is used to intercept transmissions from the Russian Molnyia satellites and other Russian telecommunications satellites.

[51] Proof Committee Hansard, Joint Standing Committee on Treaties, Reference: Pine Gap, 9 August 1999, Canberra; http://www.aph.gov.au/hansard
[52] Proof Committee Hansard, Joint Standing Committee on Treaties, Reference: Pine Gap, 9 August 1999, Canberra; http://www.aph.gov.au/hansard

Waihopai, New Zealand (173°O, 41°S)[53]
Waihopai was established in 1989. It started with one large antenna, with a diameter of 18 m, and two smaller antennae were added later. According to Hager, the antennae are trained on INTELSAT 701 in orbit above the Pacific. Official information released by the GCSB (General Communications Security Bureau) Waihopai's task is to intercept transmissions from communications satellites and to decrypt and process the signals.[54]

Since the station has only two satellite antennae, the New Zealand secret service can intercept only a small proportion of communications in the Pacific region. To serve any purpose, therefore, the station must work jointly with other stations in the region. Hager often names Geraldton in Australia as Waihopai's 'sister station'.[55]

Hong Kong (22°N, 114°O)
The station was established in the late 1970s, at the same time as the second generation of INTELSAT satellites were put in space, and was equipped with large satellite antennae. No details are available of the exact sizes. In 1994, a start was made on the decommissioning of the station; the antennae were taken to Australia. It is not clear which station (Geraldton, Pine Gap or Misawa, Japan) has taken over the Hong Kong station's tasks, which may have been divided among several stations.

5.3.2.3.2. Further stations

The roles of the following stations cannot be clearly established on the basis of the criteria referred to above:

Leitrim, Canada (75°W, 45°N)
Leitrim is part of an exchange programme between Canadian and US military units. According to the Navy, therefore, some 30 persons are stationed in Leitrim. In 1985 the first of four satellite antennae was installed, of which the two larger have a diameter of no more than roughly 12 m (estimate). According to official information, the station's task is to provide 'cryptologic rating' and to intercept diplomatic communications.

Bad Aibling, Germany (12°O, 47°N)
At present roughly 750 Americans work at the station near Bad Aibling. INSCOM (66th IG, 718th IG) which has the command, NAVSECGRU, and various AIA groups (402nd IG, 26th IOG) are stationed in Bad Aibling. The station has 14 satellite antennae, none of which has a diameter of more than 18 m. According to official information, Bad Aibling has the following tasks: 'Rapid Radio Relay and Secure Common, Support to DoD and Unified Commands, Medium and

[53] Domestic and External Security Secretariat, Department of the Prime Minister and Cabinet 'Securing our Nation's Safety', December 2000, http://www.dpmc.govt.nz/dess/securingoursafety/index.html
[54] Domestic and External Security Secretariat, Department of the Prime Minister and Cabinet: 'Securing our Nations Safety', December 2000, http://www.dpmc.govt.nz/dess/securingoursafety/index.html: 'In 1989, [...] the GCSB opened its satellite communications interception station at Waihopai, near Blenheim. [...] The signals intelligence is obtained from a variety of foreign communications and other non-communications signals, such as radar. The GCSB not only intercepts the signals, it also processes, decrypts or decodes and/or translates the information the signals contain before passing it on as a report to the appropriate Minister or government department.'
[55] *Nicky Hager,* Secret Power. New Zealands´s Role in the International Spy Network, Craig Potton Publishing (1996), 182

Longhand Common HF & Satellite, Communication Physics Research, Test and Evaluate Common Equipment'. According to Richelson, Bad Aibling is an earth station for SIGINT satellites and a listening station for transmissions from Russian telecommunications satellites. In accordance with a Department of Defense decision, the station is to be closed on 30 September 2002. Personnel will be transferred to other units.[56]

Ayios Nikolaos, Cyprus (32°O, 35°N)
Ayios Nilolaos on Cyprus is a British station. The station, which has 14 satellite antennae whose size is unknown, is manned by two units, the 'Signals Regiment Radio and the Signals Unit (RAF)'.
The station's location, close to the Arab states, and the fact that Ayios Nikolaos is the only station sited within certain footprints (above all spot beams) in this area, point to its having an important role in intelligence gathering.

Shoal Bay, Australia (134°O, 13°S)
Shoal Bay is a station run solely by the Australian Intelligence Service. The station reportedly has 10 satellite antennae; no official information is available regarding their size. Of the satellite antennae visible on photographs, the five larger ones have a maximum diameter of 8 m, and the sixth antenna visible is smaller still. According to information provided by Richelson, the antennae are trained on the Indonesian PALAPA satellites. It is not clear whether the station is part of the global system for the interception of civilian communications.

Guam, Pacific (144°O, 13°S)
Guam was established in 1898. It now houses a Naval Computer and Telecommunications Station manned by the 544th IG of the AIA and Navy soldiers. The station has at least four satellite antennae, two of which have a diameter of roughly 15 m.

Kunia, Hawaii (158°W, 21°N)
This station has been operated by NAVSECGRU and the AIA since 1993 as a Regional Security Operations Centre (RSOC). Its tasks include the provision of information and communications and cryptological support. Its broader role is not clear.

Buckley Field, Denver, Colorado, USA (104°W, 40°N)
The station was established in 1972 and is home to the 544th IG (Detachment 45). The site houses at least six satellite antennae, four of which have a diameter of roughly 20 m. The station's official task is to collect, process and analyse data about nuclear events obtained by SIGINT satellites.

Medina Annex, Texas, USA (98°W, 29°N)
Like Kunia, Medina, which was established in 1993, is an RSOC operated by NAVSECGRU and AIA units with tasks in the Caribbean.

Fort Gordon (81°W, 31°N)
Fort Gordon is also an RSOC, operated by INSCOM and the AIA (702nd IG, 721st IB, 202nd IB, 31st IS), whose tasks are unclear.

[56] Announcement of 31 May 2001 on the INSCOM homepage, http://www.vulcan.belvoir.army.mil/bas_to_close.asp

Fort Meade, USA (76°W, 39°N)
Ford Meade is the headquarters of the NSA.

5.3.3. Summary of the findings

The following conclusions can be drawn from the information collected concerning the stations and satellites and from the requirements outlined above:

1. In each footprint there are interception stations which cover at least some of the global beams and are equipped with at least one antenna with a diameter greater than 20 m. They are stations which are operated by the Americans or British or where American or British servicemen carry out intelligence activities.

2. The expansion of INTELSAT communications and the establishment, at the same time, of the corresponding interception stations show that the system is intended to provide global coverage.

3. According to official information, some of these stations have the task of intercepting transmissions from communications satellites.

4. The information regarding stations contained in the declassified documents can be regarded as proof of the existence and activities of the stations concerned.

5. Some stations are located in the areas covered by the beams or spots of several satellites, so that a large proportion of the relevant communications can be intercepted.

6. There are some other stations which, although they have no large antennae, may also be part of the system, since they can receive communications from the beams and spots. In this case, evidence other than the size of the antennae must be adduced.

7. Some of the stations are situated in immediate proximity to normal earth stations for telecommunications satellites.

5.4. The UKUSA Agreement

A SIGINT agreement signed in 1948 between the United Kingdom, the United States and Australia, Canada and New Zealand is referred to as the UKUSA Agreement.

5.4.1. The historical development of the UKUSA Agreement[57]

The UKUSA Agreement represents a continuation of the cooperation between the USA and the UK which dates back to the First World War and which became very close during the Second World War.

[57] *Christopher Andrew*, The making of the Anglo-American SIGINT Alliance in *Hayden B. Peake, Samuel Halpern* (Eds.), In the Name of Intelligence. Essays in Honor of *Walter Pforzheimer,* NIBC Press (1994), 95 -109

It was the Americans who instigated the establishment of a SIGINT alliance at a meeting with the British in London in August 1940[58]. In February 1941, US codebreakers delivered a cipher machine (PURPLE) to the United Kingdom. Cooperation in the sphere of codebreaking began in spring 1941[59]. Intelligence cooperation was stepped up in response to the joint fleet operations in the North Atlantic in summer 1941. In June 1941 the British broke the German fleet code, ENIGMA.

America's entry into the war led to SIGINT cooperation being stepped up. In 1942, US codebreakers from the Naval SIGINT Agency began work in the United Kingdom[60]. Liaison between the submarine tracking rooms in London, Washington and, from May 1943 onwards, Ottawa in Canada was so close that, according to a statement by one individual involved at the time, they worked like a single organisation[61].

In spring 1943 the BRUSA-SIGINT Agreement was signed, and personnel were exchanged. The agreement primarily concerns the division of work and its main substance is summarised in the first three paragraphs: they cover the exchange of all information obtained by means of the discovery, identification and interception of signals and the cracking of codes and encryption processes. The Americans were primarily responsible for Japan, the British for Germany and Italy[62].

Following the war, the UK was the prime mover behind the continuation of a SIGINT alliance. The foundations were laid in the course of a world tour undertaken in spring 1945 by British intelligence agents (including Sir Harry Hinsley, whose books are used as source material in the articles quoted in the footnotes). One aim was to transfer SIGINT personnel from Europe to the Pacific to take part in the war against Japan. In that connection, an agreement was reached to provide the Australian intelligence services with resources and personnel (British). The intelligence agents returned to the USA via New Zealand and Canada.

In September 1945 Truman signed a top-secret memorandum whose provisions formed the cornerstone of a peacetime SIGINT alliance[63]. Immediately thereafter, negotiations on an

---

[58] *Christopher Andrew,* The making of the Anglo-American SIGINT Alliance, ibidem, 99: 'At a meeting in London on 31 August 1940 between the British Chiefs of Staff and the American Military Observer Mission, the US Army representative, Brigadier General George V. Strong, reported that 'it had recently been arranged in principle between the British and the United States Governments that periodic exchange of information would be desirable,' and said that 'the time had come or a free exchange of intelligence'. (quoted from COS (40)289, CAB 79/6, PRO. *Smith*, The Ultra Magic Deals, 38, 43-4. *Sir F.H. Hinsley*, et al., British Intelligence in the Second World War, Vol. I, 312-13).

[59] *Christopher Andrew* The making of the Anglo-American SIGINT Alliance, ibidem,100: ' In the spring of 1941, Steward Menzies, the Chief of SIS, appointed an SIS liaison officer to the British Joint Services Mission in Washington, Tim O´Connor, …, to advice him on cryptologic collaboration'.

[60] *Christopher Andrew,*The making of the Anglo-American SIGINT Alliance, ibidem, 100 (*Sir F.H. Hinsley*, et al., British Intelligence in the Second World War, Vol. II, 56)

[61] *Christopher Andrew,*The making of the Anglo-American SIGINT Alliance, ibidem, 101 (*Sir F.H. Hinsley*, et al., British Intelligence in the Second World War, Vol. II, 48)

[62] *Christopher Andrew,*The making of the Anglo-American SIGINT Alliance, ibidem, 101-2: Interviews with Sir F.H. Hinsley, 'Operations of the Military Intelligence Service War Department London (MIS WD London),' 11 June 1945, Tab A, RG 457 SRH-110, NAW

[63] *Harry S. Truman*, Memorandum for the Secretaries of the State, War and the Navy, 12 Sept. 1945: 'The Secretary of War and the Secretary of the Navy are hereby authorised to direct the Chief of Staff, U.S. Army and the Commander in Chief, U.S. Fleet; and Chief of Naval Operations to continue collaboration in the field of communication intelligence between the United States Army and Navy and the British, and to extend, modify or discontinue this collaboration, as determined to be in the best interests of the United States.' (quoted from *Bradley F.*

agreement opened between the British and Americans. In addition, a British delegation made contact with the Canadian and Australians with a view to discussing their involvement. In February and March 1946 a top-secret Anglo-American SIGINT conference took place at which the details of an alliance were discussed. The British were authorised by the Canadians and Australians to act on their behalf. The conference produced what was still a classified agreement, running to some 25 pages, which laid down the detailed arrangements for a SIGINT agreement between the United States and the British Commonwealth. Further discussions took place during the two following years, culminating in the signing of the definitive text of the UKUSA Agreement in June 1948[64].

5.4.2. Evidence for the existence of the agreement

5.4.2.1. 1999/2000 annual report of the UK Intelligence and Security Committee

For a long time, the signatory states refused officially to acknowledge the existence of the UKUSA Agreement. However, the annual report of the Intelligence and Security Committee, the UK's parliamentary monitoring body, refers explicitly to the agreement: 'The quality of intelligence gathered clearly reflects the value of the close co-operation under the UKUSA agreement. A recent illustration of this occurred when the US National Security Agency's (NSA) equipment accidentally failed and for some three days US customers, as well as GCHQ's normal UK customers, were served directly from GCHQ'.[65]

5.4.2.2. Publication of the New Zealand Department of the Prime Minister

A publication of the New Zealand Department of the Prime Minister from the year 2000, dealing with the management of the New Zealand's security and intelligence services, also refers clearly to the agreement: .'The operation of the GCSB is directed solely by the New Zealand Government. It is, however, a member of a long-standing collaborative international partnership for the exchange of foreign intelligence and the sharing of communications security technology. The other members of the partnership are the USA's National Security Agency (NSA), the UK's Government Communications Headquarters (GCHQ) Australia's Defence Signals Directorate (DSD), and Canada's Communications Security Establishment (CSE). New Zealand gains considerable benefit from this arrangement, as it would be impossible for New Zealand to generate the effectiveness of the five nation partnership on its own'.[66]

Moreover, there is further evidence of the agreement's existence.

Smith, The Ultra-Magic Deals and the Most Secret Special Relationship (Novato, Ca: Presidio 1993))

[64] *Christopher Andrew*, The making of the Anglo-American SIGINT Alliance in Hayden, H. Peake and Samuel Halpern Eds, In the Name of Intelligence. Essays in Honor of Walter Pforzheimer (NIBC Press 1995) 95 –109: Interviews with Sir Harry Hinsley, March/April 1994, who did a part of the negotiations; Interviews with Dr. Louis Tordella, Deputy Director of NSA from 1958 to 1974, who was present at the signing.

[65] Intelligence and Security Committee Annual Report 1999-2000. Presented to Parliament by the Prime Minister by Command of Her Majesty, November 2000, 8, 14

[66] Domestic and External Secretariat of the Department of the Prime Minister and Cabinet of New Zealand, Securing our Nation's Safety. How New Zealand manages its security and intelligence agencies (2000).

5.4.2.3. The Navy acronym list

According to the US Navy[67], UKUSA stands for 'United Kingdom-USA' and refers to a '5-nation SIGINT agreement'.

5.4.2.4. Statement by the Head of the DSD

The Head of the Australian Intelligence Service (DSD) confirmed the existence of the agreement in an interview: according to the information he gave, the Australian Secret Service cooperates with other overseas intelligence agencies under the UKUSA Agreement[68].

5.4.2.5. Report by the Canadian Parliamentary Security and Intelligence Committee

This report describes how Canada cooperates with some of its closest and longest-standing allies in the intelligence sphere. The report names the allies concerned: the United States (NSA), the United Kingdom (GCHQ), Australia (DSD) and New Zealand (GCSB). The report does not name the agreement.

5.4.2.6. Statement by the former Deputy Director of the NSA, Dr Louis Torella

In an interview with Christopher Andrew, a professor at Cambridge University, conducted in November 1987 and April 1992, the former Deputy Director of the NSA, Dr Louis Torella, who was present when the agreement was signed, confirmed that it does exist[69].

5.4.2.7 Letter from the former Head of HCHQ, Joe Hooper

The former Head of GCHQ, Joe Hooper, refers to the UKUSA Agreement in a letter of 22 July 1969 to the former Director of the NSA, Marshall S. Carter.

5.4.2.8. Rapporteur's discussion partners

Your rapporteur has spoken about the agreement with several persons who, by virtue of their duties, must be aware of the UKUSA Agreement and its substance. In all cases, the existence of the agreement was indirectly confirmed by the nature of the answers given.

5.5. Evaluation of declassified US documents

5.5.1. Nature of documents

Under the 1966 Freedom of Information Acts (5 USC § 552) and the Department of Defense's 1997 FOIA Regulation 5400.7-R, formerly classified documents were declassified and thus made available to the public.

[67] 'Terms/Abbreviations/Acronyms' published by the US Navy and Marine Corps Intelligence Training Centre (NMITC) at http://www.cnet.navy.mil/nmitc/training/u.html
[68] *Martin Brady*, Head of the DSD, letter of 16.3.1999 to Ross Coulthart, Sunday Program Channel 9
[69] *Christopher Andrew* 'The growth of the Australian Intelligence Community and the Anglo-American Connection', 223-4.

The documents concerning the National Security Archive, founded in 1985 at George Washington University in Washington DC, are accessible to the public. The author Jeffrey Richelson, a former member of the National Security Archive, has published 16 documents on the Internet which give an insight into the emergence, development, management and mandate of the National Security Agency (NSA).[70] In two of these documents, ECHELON is named. These documents have repeatedly been cited by various authors writing about ECHELON as evidence for the existence of the ECHELON global espionage system. The documents made available by Richelson also include some which confirm the existence of the National Reconnaissance Office and its function as a manager and operator of intelligence satellites.[71] Following our conversation with Jeffrey Richelson in Washington he forwarded further declassified documents to the Temporary Committee. Those relevant to our investigations have been taken into account here.

5.5.2. Content of documents

The documents contain fragmentary descriptions of or references to the following topics:

5.5.2.1. Purpose and structure of the NSA (Documents 1, 2b, 4, 10 and 16)

In National Security Council Intelligence Directive 9 (NSCID 9) of 10 March 1950[72] the term 'foreign communications' is defined for COMINT purposes: it comprises **any government communications in the widest sense (not only military) and all other communications which might contain information of military, political, scientific or economic value.**

The Directive (NSCID 9 rev, 29.12.1952)[73] expressly states that the FBI alone is responsible for internal security.

The Department of Defense (DoD) Directive of 23 December 1971[74] on the NSA and the Central Security Service (CSS) outlines the concept for the NSA as follows:

- The NSA is a separately organised office within the DoD headed by the Secretary of Defence;
- The NSA's task is firstly to fulfil the USA's SIGINT mission, and secondly to provide secure communications systems for all departments and offices;
- The NSA's SIGINT activities do not cover the production and distribution of processed intelligence: this is the sphere of other departments and offices.

The 1971 DoD Directive also sketches out the structure of the NSA and CSS.

In its statement to the House Permanent Select Committee on Intelligence on 12 April 2000[75], Gen. Michael Hayden, the NSA Director, defined the NSA's tasks as follows:

---

[70] *Jeffrey T.Richelson*, The National Security Agency Declassified, National Security Archive Electronic Briefing Book No 24, George Washington University http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB23/index.html
[71] *Jeffrey T. Richelson,* The National Security Agency Declassified, National Security Archive Electronic Briefing Book No 24, George Washington University http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB35/index.html
[72] Document 1. NSCID 9, 'Communications Intelligence,' March 10 1950.
[73] Document 2b. National Security Council Intelligence Directive No 9, Communications Intelligence, December 29 1952
[74] Document 4. Department of Defense Directive S-5100.20, 'The National Security Agency and the Central Security Service,' December 23 1971

- Collecting foreign communications for the military and for policymakers by means of electronic surveillance;
- Supplying intelligence for US Government consumers about international terrorism, drugs and arms proliferation;
- The NSA does not have the task of collecting all electronic communications.
- The NSA may only pass on information to recipients authorised by government, not direct to US firms.

In a memorandum by Vice-Admiral W.O. Studeman of the US Navy on behalf of the Government on 8 April 1992[76], reference was made to the increasingly global access of the NSA in addition to 'support of military operations'.

5.5.2.2. Powers of the Intelligence Agencies (Document 7)[77]

It is clear from US Signals Intelligence Directive 18 (USSID 18) that both cable and radio signals are intercepted.

5.5.2.3. Cooperation with other services (Documents 2a and 2b)

The duties of the US Communications Intelligence Board include monitoring all 'arrangements' with foreign governments in the COMINT field. One of the tasks of the NSA Director is to arrange all contacts with foreign COMINT services.[78]

5.5.2.4. Mention of units active in 'ECHELON sites' (Documents 9 and 12)

The NAVSECGRU Instructions C5450.48A[79] describe the duties, function and purpose of the Naval Security Group Activity (NAVSECGRUACT), 544th Intelligence Group, in Sugar Grove, West Virginia. They state that one particular task is to 'maintain and operate an ECHELON site'; they also mention that one task is the processing of intelligence information.

In the document 'History of the Air Intelligence Agency – 1 January to 31 December 1994[80] the Air Intelligence Agency (AIA), Detachment 2 and 3, is mentioned under the heading 'Activation of ECHELON Units'.

---

[75] Document 16. Statement for the Record of NSA Director Lt Gen Michael V. Hayden, USAF before the House Permanent Select Committee on Intelligence, April 12 2000.
[76] Document 10. Farewell from Vice Admiral William O. Studeman to NSA Employees, April 8 1992.
[77] Document 7. United States Signals Intelligence Directive [USSID] 18, 'Legal Compliance and Minimization Procedures,' July 27 1993.
[78] Document 2a. Memorandum from President Harry S. Truman to the Secretary of State, the Secretary of Defense, Subject: Communications Intelligence Activities, October 24 1952.
Document 2b. National Security Council Intelligence Directive No. 9, Communications Intelligence, December 29 1952.
[79] Document 9. NAVSECGRU Instruction C5450.48A, Subj: Mission, Functions and Tasks of Naval Security Group Activity (NAVSECGRUACT) Sugar Grove, West Virginia, September 3 1991.
[80] Document 12. 'Activation of Echelon Units,' from History of the Air Intelligence Agency, 1 January - 31 December 1994, Volume I (San Antonio, TX: AIA, 1995).

These documents do not give any information on what an 'ECHELON site' is, what is done at an 'ECHELON site', or what the code name ECHELON stands for. These documents do not reveal anything about the UKUSA Agreement.

5.5.2.5. Mention of Stations (Documents 6, 9 and 12, new documents)

- Sugar Grove, West Virginia, named as SIGINT station in the NAVSECGRU Instructions C5450.48A[81]
- Misawa Air Base, Japan, named as SIGINT station in History of the Air Intelligence Agency – 1 January to 31 December 1994[82] and in description of the activities of the Naval Security Group in Department of the Navy documents[83]
- Sabana Seca in Puerto Rico, ibid. and in description of the activities of the Naval Security Group in Department of the Navy documents[84]
- Guam, named as SIGINT station, ibid.
- Yakima, Washington, named as SIGINT station, ibid.
- Fort Meade, Maryland; a COMINT report by the NSA of 31 August 1971 from Fort George G. Meade, Maryland confirms the COMINT activities there[85]
- Menwith-Hill, United Kingdom, description of the activities of the Naval Security Group in Department of Navy documents[86]
- Bad Aibling, Germany, description of the activities of the Naval Security Group in Department of Navy documents[87]
- Medina, Texas, description of the activities of the Naval Security Group in Department of Navy documents[88]
- Kunia, Hawaii, description of the activities of the Naval Security Group in Department of Navy documents[89]

5.5.2.6. Protection of the privacy of US citizens (Documents 7, 7 a to f, 9, 11 and 16)

The NAVSECGRU Instructions C5450.48A state that the privacy of citizens must be protected[90].

Various documents state that the privacy of US citizens must be protected and how this is to be done (Baker, General Counsel, NSA, letter of 9 September 1992, US Signals Intelligence Directive (USSID) 18, 20 October 1980, and various supplements.[91]

---

[81] Document 9. NAVSECGRU Instruction C5450.48A, Subj: Mission, Functions and Tasks of Naval Security Group Activity (NAVSECGRUACT) Sugar Grove, West Virginia, September 3, 1991.
[82] Document 12. 'Activation of Echelon Units,' from History of the Air Intelligence Agency, 1 January - 31 December 1994, Volume I (San Antonio, TX: AIA, 1995).
[83] Department of the Navy, Naval Security Group Instruction C5450.32E, 9.5.1996
[84] Naval Security Group Instruction C5450.33B, 8.8.1996
[85] COMINT report by the NSA from Fort George G. Meade, Maryland of 31 August 1972
[86] Department of the Navy, Fact and Justification Sheet for the Establishment of U.S. Naval Security Group Activity of 23.2.1995 and Department of the Navy, Naval Security Group Instruction C5450.62, 30.1.1996
[87] Department of the Navy, Naval Security Group Instruction C5450.63, 25.10.1995
[88] Department of the Navy, Naval Security Group Instruction C5450.60A, 8.4.1996
[89] Naval Security Group Instruction C5450.55B, 8.8.1996
[90] Document 9. NAVSECGRU Instruction C5450.48A, Subj: Mission, Functions and Tasks of Naval Security Group Activity (NAVESCGRUACT) Sugar Grove, West Virginia, 3 September 1991
[91] Dissemination of US Government Organisations and Officials, Memorandum 5 February 1993; Reporting Guidance on References to the First Lady, 9 July 1993; Reporting Guidance on Former President Carter's

5.5.2.7. Definitions (Documents 4, 5a and 7)

The Department of Defense Directive of 23 December 1971[92] provides precise definitions of SIGINT, COMINT, ELINT and TELINT, as does the National Security Council Intelligence Directive No 6 of 17 February 1972.[93]

According to these, COMINT means the collection and processing of foreign communications (passed by electromagnetic means) up to and including the interception and processing of unencrypted written communications, press and propaganda unless encrypted.

5.5.3. Summary

1. As long as 50 years ago there was interest in information not only from the political and security spheres but also from the fields of science and economics.
2. The documents prove that the NSA works together with other services in the field of COMINT.
3. The documents which reveal information about how the NSA is organised, what tasks it has and that it is responsible to the Department of Defense, do not add any essential information beyond what can be gathered from publicly accessible sources on the NSA home page.
4. Cable communications may be intercepted.
5. The 544th Intelligence Group and Detachment 2 and 3 of the Air Intelligence Agency are involved in the collection of intelligence information.
6. The term 'ECHELON' appears in a number of contexts.
7. Sugar Grove in West Virginia, Misawa Air Base in Japan, Puerto Rica (i.e. Sabana Seca), Guam, and Yakima in Washington State are named as SIGINT stations.
8. Further stations at which the Naval Security Group is active are named without being identified as SIGINT stations.
9. The documents provide information on how the privacy of American citizens should be protected.

The documents do not constitute proof, but provide compelling clues which enable conclusions to be drawn when taken in conjunction with other evidence.

Involvement in the Bosnian Peace Process, 15 December 1994; Understanding USSID 18, 30 September 1997; USSID 18 Guide, 14 February 1998.
NSA/US Identities in SIGINT, March 1994: Statement for the record of NSA Director Lt Gen Michael V. Hayden, USAF, 12 April 2000.

[92] Document 4. Department of Defense Directive S-5100.20, 'The National Security Agency and the Central Security Service,' December 23 1971

[93] Document 5a. NSCID 6, 'Signals Intelligence,' February 17 1972.

5.6. Information from authors and journalists specialised in this field

5.6.1. Nicky Hager's book

The ECHELON system was first described in detail in the book 'Secret Powers – New Zealand's role in the international spy network', published in 1996 by the New Zealand author Nicky Hager.

He draws on interviews with more than 50 persons who were employed by the New Zealand intelligence service, GCSB, or otherwise involved in intelligence activities. He also analysed a wide range of documents from national archives, newspapers and other published sources. According to Hager, the global interception system is referred to as ECHELON, and the network computers as ECHELON Dictionaries.

According to Hager, the origins of cooperation between intelligence services under the UKUSA Agreement can be traced back to 1947, when, following their cooperation in the war, the UK and USA concluded an agreement on continuing COMINT activities on a joint basis around the globe, under which the two countries were to cooperate on the creation of an interception system providing the maximum possible global coverage, share the special installations required and the associated costs and pool the fruits of their labours. Canada, Australia and New Zealand subsequently signed up to the UKUSA agreement.

Hager says that interception of satellite communications is the core activity of the **current** system. The interception by ground stations of messages sent via Intel satellites – the first global satellite communication system[94] - began in the 1970s. Such messages are then searched by computer for specific keywords and/or addresses in order to filter out the relevant communications. Surveillance activity was later extended to other satellites, such as those of Inmarsat[95], which concentrated on maritime communications.

In his book, Hager points out that the interception of satellite communications represents only a small, albeit important, part of the eavesdropping system, for there are also numerous facilities for monitoring microwave and cable links, although these are less well documented and their existence is more difficult to prove, since, unlike ground stations, they are rather inconspicuous. ECHELON is thus synonymous with a global eavesdropping system.

In his statement to the Temporary Committee, made on 24 April 2001, Hager emphasised that the interception system was not all-powerful. Since the limited resources had to be used as effectively as possible, not all communications could be intercepted, but rather only those likely to offer up important information. For that reason, the communications targeted were those of political and diplomatic interest. If communications were intercepted with a view to obtaining economic intelligence, the information concerned the macro - rather than the microeconomic sphere.

[94] Intelsat homepage, http://www.intelsat.int/index.htm
[95] Inmarsat homepage, http://www.inmarsat.org/index3.html

As far as the interception system's operating methods were concerned, each partner state had its own list of search words on the basis of which communications were intercepted. In addition, however, communications were screened for keywords entered into the system by the USA using 'dictionary managers'. The British therefore had no control over the screening process and had no idea what information was collected in Morwenstow, since it was forwarded directly to the USA.

In that connection, Hager emphasised the risk posed to continental Europe by the British interception stations. Citing several examples, he pointed out that the UKUSA partner states were spying on allies and trading partners in the Pacific. The only countries not being spied on were the UKUSA partner states themselves. In Hager's view, like their New Zealand counterparts the British secret services would probably be very loath to call the UKUSA partnership into question by refusing to cooperate and intercept communications originating from continental Europe. There would be no reason for the United Kingdom to forfeit information of interests to its intelligence services, and, since that information would always remain secret, espionage under the UKUSA Agreement would not rule out an official policy of loyalty vis-à-vis Europe.

5.6.2. Duncan Campbell

In his many publications the British journalist Duncan Campbell draws on the work of Hager and Richelson, on conversations with former intelligence service staff and on other research. According to his statements, ECHELON is part of the global system which intercepts and analyses international satellite communications. Each partner state uses 'dictionary' computers which screen the intercepted messages for keywords.

In STOA Study 2/5 of 1999, which provides an in-depth analysis of the technical aspects, Campbell describes in detail how any medium used for transmitting information can be intercepted. In one of his latest writings, however, he makes it clear that even ECHELON has its limits and that the initial view that total monitoring of communications was possible has turned out to be erroneous. 'Neither ECHELON nor the signals intelligence ('SIGINT') system of which it is part can do this. Nor is equipment available with the capacity to process and recognise the content of every speech message or telephone call.' [96]

In his statement to the Temporary Committee, made on 22 January 2001, Campbell expressed the view that the USA used its intelligence services to help US firms win contracts. Relevant information was passed on to firms via the CIA with the assistance of the Advocacy Center and the Office of Executive Support in the Department of Commerce. In support of this argument he put forward documents providing evidence of intervention by the Advocacy Center to the benefit of US firms; moreover, much of the information concerned can be found on the homepage of the Advocacy Center.[97] The claim that the success of the Advocacy Center is based on the interception of communications is speculation and is not supported by the documents.

---

[96] *Duncan Campbell*, Inside ECHELON. The history, structure and function of the global surveillance system known as ECHELON, 1

[97] Homepage of the Advocacy Center, http://www.ita.doc.gov/td/advocacy/index.html
In the course of his visit to Washington DC your rapporteur wanted to give the Advocacy Center an opportunity to respond to these accusations. However, a pre-arranged meeting was cancelled by the Department of Commerce at short notice.

Campbell emphasised that the interception capabilities of several European countries (e.g. Switzerland, Denmark, France) had increased substantially in recent years. The intelligence sector had also seen an expansion in bilateral and multilateral cooperation.

5.6.3. Jeff Richelson

The US author, Jeffrey Richelson, a former member of the National Security Archives, has made available on the Internet 16 previously classified documents which give an insight into the inception, development, management and remit of the National Security Agency[98].

In addition, he is the author of various books and articles on the intelligence activities of the USA. In his work he draws on many declassified documents, the research carried out by Hager and his own research. During his meeting with the delegation from the Temporary Committee, held in Washington DC on 11 May 2001, he stated that ECHELON referred to a computer network used to filter data which was then exchanged between intelligence services.

In his 1985 book 'The Ties That Bind'[99] he describes in detail the negotiations which led up to the signing of the UKUSA Agreement and the activities under that agreement of the secret services of the USA, the United Kingdom, Canada, Australia and New Zealand.

In his very comprehensive 1999 book 'The US Intelligence Community'[100] he gives a survey of the USA's intelligence activities and describes the organisational structure of the intelligence services and their methods of collecting and analysing information. In Chapter 8 of the book he examines in detail the SIGINT capabilities of the intelligence services and describes some earth stations. In Chapter 13 he outlines the USA's relations with other intelligence services, for example under the UKUSA Agreement.

In his article entitled 'Desperately Seeking Signals'[101], which appeared in 2000, he gives brief details of the substance of the UKUSA Agreement, names installations used to intercept transmissions from communications satellites and outlines the scope for and the limits on the interception of civilian communications.

5.6.4. James Bamford

US author James Bamford, whose work is based both on archive research and the questioning of intelligence service staff, was one of the first people to tackle the subject of the MSA's SIGINT activities As long ago as 1982 he published the book 'The Puzzle Palace'[102], chapter 8 of which, entitled 'Partners', describes the UKUSA Agreement in detail. According to his new book, 'Body of Secrets'[103], which builds on the findings outlined in 'The Puzzle Palace', the computer network linking the intelligence services is known as 'Platform'. ECHELON is the name of the software

[98] *Jeffrey T. Richelson*, The National Security Agency Declassified, National Security Archive Electronic Briefing Book No 24, George Washington University, http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB23/index.html
[99] *Jeffrey T. Richelson, Desmond Ball,* The Ties That Bind, Boston UNWIN HYMAN (1985)
[100] *Jeffrey T. Richelson,* The U.S. Intelligence Community[4], Westview Press (1999)
[101] *Jeffrey T. Richelson,* Desperately Seeking Signals, The Bulletin of the Atomic Scientists, Vol. 56, No. 2/2000,
[102] *James Bamford,* The Puzzle Palace, Inside the National Security Agency, America's most secret intelligence organization (1983)
[103] *James Bamford,* Body of Secrets. Anatomy of the Ultra-Secret National Security Agency. From the Cold War Through the Dawn of a New Century, Doubleday Books (2001)

used in all the relevant stations, providing for uniform processing of data and direct access to the data held by other intelligence services[104]. In the subsequent chapters, however, he also uses the term ECHELON to denote the interception system set up under the UKUSA Agreement.

In 'Body of Secrets', and in the chapter of most relevance to the work of the Temporary Committee, entitled 'Muscle', Bamford gives a historical survey of the development of communications surveillance by the NSA and describes the scope of the system, the way the UKUSA partnership operates and its objectives. He emphasises that, according to interviews conducted with dozens of current and former NSA employees, the NSA is at present not involved in the work of gathering competitive intelligence.

He confirmed this statement when giving evidence to the Temporary Committee on 23 April 2001. The NSA could only be given the task of gathering competitive intelligence on the basis of a clear political decision taken at the very highest level, a decision which has thus far not been taken. In the course of 20 years' research, Bamford had never uncovered evidence of the NSA passing on intelligence to US firms, even though it intercepts communications from private firms, for example with a view to monitoring compliance with embargoes.

According to Bamford, the main problem for Europe is not the issue of whether the ECHELON system steals firms' business secrets and passes them on to competitors, but rather that of the violation of the fundamental right to privacy. In 'Body of Secrets' he describes in detail how the protection of 'US persons' (i.e. US citizens and persons legally resident in the USA) has developed and makes clear that at least internal restrictions have been laid down in respect of other UKUSA residents. At the same time, he points out that other persons enjoy no protection, that there is no requirement to destroy data concerning such persons, and that the NSA's data storage capacities are unimaginably huge.

However, Bamford also emphasises the limits of the system, which stem from the fact that, firstly, only a small proportion of international communications are now transmitted via satellites - transmissions via fibreoptic cable are much more difficult to intercept - and, secondly, that the NSA has only limited capacities when it comes to the final analysis of intercepted communications. Moreover, those capacities must be set against an ever-increasing volume of communications, transmitted in particular via the Internet.

5.6.5. Bo Elkjaer and Kenan Seeberg

These two Danish journalists told the Temporary Committee on 22 January 2001 that ECHELON was already very advanced in the 1980s. Denmark, which greatly expanded its interception capabilities in the 1990s, has been cooperating with the USA since 1984.

Echoing their article in Ekstra Bladet[105], in which they referred to an illustrated lecture (25 slides) given by an unnamed officer of the 544th Intelligence Group of the Air Intelligence Agency, they claimed that various NGOs (including the Red Cross) were also ECHELON targets.

---

[104] *James Bamford*, Body of Secrets, Anatomy of the Ultra-Secret National Security Agency, From the Cold War Through the Dawn of a New Century, Doubleday Books (2001), 404.

[105] *Bo Elkjaer, Kenan Seeberg*, ECHELON singles out the Red Cross, A bombshell in the surveillance scandal: The organization is a possible surveillance target, Ekstra Bladet, Denmark, 8.3.2000, http://cryptome.org/echelon-

5.7. Statements by former intelligence service employees

5.7.1. Margaret Newsham (former NSA employee)[106]

Margaret Newsham was employed from 1974 to 1984 by Ford and Lockheed and says she worked for the NSA during that period. She had been trained for her work at NSA Headquarters at Fort George Meade in Maryland, USA, and had been deployed from 1977 to 1981 at Menwith Hill, the US ground station on UK territory. There she established that a conversation conducted by US Senator Strohm Thurmond was being intercepted. As early as 1978, ECHELON was capable of intercepting telecommunications messages to and from a particular person via satellite.

As regards her role in the NSA, she was responsible for designing systems and programs, configuring them and preparing them for operation on powerful computers. The software programs were named SILKWORTH and SIRE, whilst ECHELON was the name of the network.

5.7.2. Wayne Madsen (former NSA employee)

Wayne Madsen[107], former NSA employee, also confirms the existence of ECHELON. He is of the opinion that economic intelligence gathering has top priority and is used to the advantage of US companies. He fears in particular that ECHELON could spy on NGOs such as Amnesty International or Greenpeace. He argues that the NSA had to concede that it held more than 1000 pages of information on Princess Diana, because her conduct ran counter to US policy, owing to her campaign against land mines.

During his meeting with the committee delegation in Washington DC Madsen expressed particular concern at the risks to the privacy of European citizens posed by the global espionage system.

5.7.3. Mike Frost (former Canadian secret service employee)

Mike Frost worked for more than 20 years for the CSE, the Canadian secret service[108]. The listening post in Ottawa was just one part of a worldwide network of spy stations.[109] In an interview with CBS, he said that all over the world, every day, telephone conversations, e-mails and faxes are monitored by ECHELON, a secret government surveillance network.[110] This also included civilian communications. In an interview he gave for an Australian TV channel, he said by way of example that the CSE actually had entered the name and telephone number of a woman in a database of possible terrorists because she had used an ambiguous phrase in a harmless telephone conversation with a friend. When searching through intercepted

---

red.htm

[106] *Bo Elkjaer, Kenan Seeberg*, ECHELON was my baby – Interview with Margaret Newsham, Ekstra Bladet, 17.1.1999

[107] NBC TV interview '60 Minutes', 27.2.2000; http://cryptome.org/echelon-60min.htm

[108] Communication Security Establishment, subordinate to the Canadian Ministry of Defense, engaged in SIGINT

[109] NBC TV interview '60 Minutes', 27.2.2000; http://cryptome.org/echelon-60min.htm

[110] *Florian Rötzer*, Die NSA geht wegen ECHELON an die Öffentlichkeit; http://www.heise.de/bin/tp/issue/download.cgi?artikelnr=6633&rub_ordner=special

communications, the computer had found the keyword and reproduced the conversation. The analyst was unsure and therefore recorded her personal details.[111]

The intelligence services of the UKUSA states also helped each other by spying on each other's behalf so that at least local intelligence services could not be accused of anything. For instance, GCHQ asked the CSE to spy on two British government ministers when Prime Minister Thatcher wanted it to tell her if they were on her side.[112]

5.7.4. Fred Stock (former Canadian secret service employee)

Fred Stock says he was expelled from CSE, the Canadian secret service, in 1993 because he had criticised the new emphasis on economic intelligence and civil targets. The communications intercepted contained information on trade with other countries, including negotiations on NAFTA, Chinese purchases of cereals and French arms sales. Stock says the service also routinely received communications concerning environmental protests by Greenpeace vessels on the high seas.[113]

5.8. Information from government sources

5.8.1. USA

James Woolsey, the former director of the CIA, said at a press conference[114] he gave at the request of US State Department, that the USA did conduct espionage operations in continental Europe. However, 95% of 'economic intelligence' was obtained by evaluating publicly accessible information sources, and only 5% came from stolen secrets. Espionage was used to secure economic intelligence from other countries where compliance with sanctions and dual-use goods were concerned, and in order to combat bribery in connection with the award of contracts. Such information is not, however, passed to US companies. Woolsey stressed that, even if espionage yielded economically usable intelligence, it would take an analyst a very long time to analyse the large volume of available information, and that it would be wrong to use their time on spying on friendly trading partners. He also pointed out that, even if they did so, complex international interlinkages would make it difficult to decide which companies were US companies and thus should be allowed to have the information.

5.8.2. UK

Answers to various questions in the House of Commons[115] reveal that the station at RAF Menwith Hill is owned by the UK Ministry of Defence, but is made available to the US Department of Defense, specifically the NSA[116], which provides the chief of station,[117] as a communications facility.[118] In mid-2000, there were 415 US military, 5 UK military, 989 US civilian and 392 UK civilian personnel working at RAF Menwith Hill, excluding GCHQ staff

[111] NBC TV interview '60 Minutes', 27.2.2000; http://cryptome.org/echelon-60min.htm
[112] Interview on the Australian Channel 9 on 23.3.1999;
http://www.geocities.com/CapitolHill/Senate/8789/sunday1.htm
[113] *Jim Bronskill*, Canada a key snooper in huge spy network, Ottawa Citizen, 24.10.2000,
http://www.ottawacitizen.com/national/990522/2630510.html
[114] *James Woolsey*, Remarks at the Foreign Press Center, Transcript, 7.3.2000, http://cryptome.org/echelon-cia.htm
[115] Commons Written Answers, House of Commons Hansard Debates
[116] 12.7.1995.
[117] 25.10.1994
[118] 3.12.1997

present on the site.[119] The presence of US military personnel is governed by the North Atlantic Treaty and special confidential[120] administrative arrangements appropriate to the relationship which exists between the governments of the UK and the USA for the purposes of common defence.[121] The station is an integral part of the US Department of Defense's worldwide network which supports the interests of the UK, the USA and NATO.[122]

In the Intelligence and Security Committee's 1999/2000 annual report, emphasis is specifically placed on the value of the close cooperation under the UKUSA Agreement, as reflected in the quality of the intelligence gathered. It is pointed out in particular that when the NSA's equipment was out of action for some three days, US customers as well as UK customers were served direct from GCHQ.[123]

5.8.3. Australia[124]

Martin Brady, Director of the Australian intelligence service DSD[125], confirmed in a letter to the 'Sunday' programme on Australia's Channel 9 that DSD cooperated with other intelligence services as part of the UKUSA Agreement. In the same letter, he stressed that all Australia's intelligence facilities were operated by Australian services alone or jointly with US services. Where use of such facilities is shared, the Australian Government has full knowledge of all activities and Australian personnel is involved at all levels.[126]

5.8.4. New Zealand

As already outlined under 5.4.2.2. above, a document published by the New Zealand Department of the Prime Minister in 2000, which deals with the role of the national security and intelligence services refers explicitly to the parnership between the intelligence services of the USA, the UK, Canada, Australia and New Zealand and emphasises the benefits for New Zealand[127].

5.8.5. Netherlands

On 19 January 2001, the Netherlands Minister for Defence presented a report to the Netherlands Parliament on technical and legal aspects of the global surveillance of modern telecommunications systems.[128] In it, the Netherlands Government takes the view that, although

[119] 12.5.2000
[120] 12.7.1995
[121] 8.3.1999, 6.7.1999
[122] 3.12.1997
[123] Intelligence and Security Committee (UK), Annual Report 1999-2000, para. 14, presented to the Commons by the Prime Minister in November 2000.
[124] *Martin Brady*, Director of the DSD, letter of 16.3.1999 to Ross Coulthart, Sunday Program Channel 9 http://sunday.ninemsn.com/01_cover_stories/transcript_335.asp; http://sunday.ninemsn.com/01_cover_stories/article_335.asp
[125] Defence Signals Directorate, Australian intelligence service engaged in SIGINT
[126] Letter of 16.3.1999 from Martin Brady, Director of the DSD, to Ross Coulthart, 'Sunday' programme; see also: http://sunday.ninemsn.com/01_cover_stories/transcript_335.asp; http://sunday.ninemsn.com/01_cover_stories/article_335.asp
[127] Domestic and External Secretariat of the Department of the Prime Minister and Cabinet of New Zealand, Securing our Nation's Safety. How New Zealand manages its security and intelligence agencies (2000)
[128] Brief aan de Tweede Kamer betreffende 'Het grootschalige afluisteren van moderne telecommunicatiesystemen', 19.1.2001

it had no information of its own on this matter, it was highly likely, on the basis of available third-party information, that the ECHELON network did exist, but that there were also other systems with the same capabilities. The Netherlands Government came to the conclusion that global interception of communications systems was not confined to countries involved in the ECHELON system, but was also carried on by government authorities of other countries.

5.8.6. Italy

Luigi Ramponi, former director of SISMI, the Italian intelligence service, leaves no room for doubt in the interview he gave for 'Il Mondo' that ECHELON does exist.[129] Ramponi says explicitly that, as Head of SISMI, he knew of ECHELON's existence. Since 1992, he had been kept in the picture about intensive interception of low-, medium- and high frequencies. When he joined SISMI in 1991, most dealings were with the UK and the USA.

5.9. Questions to the Council and Commission

On 17 February 1998 the MEP Elly Plooj-van Gorsel[130] tabled a first comprehensive question to the Council on the STOA report and the existence of a global inception system, operated by the USA and with the involvement of the United Kingdom, and on any resulting damage to the commercial interests of European firms. Many further questions on this topic followed.[131] The Council Presidency replied that the Council itself had no relevant information, that it was not involved in such matters and could therefore give no replies.

The similar questions to the European Commission[132] received the following response from that institution: it was aware of the report, but there was no evidence that a Member State had violated the EC Treaty in that respect and no complaints had been submitted.[133] However, the Commission was adopting a vigilant approach, would defend all Community interests and would make further efforts to improve the security of its data network.[134] At the plenary sitting of

[129] *Francesco Sorti*, Dossier esclusivo. Caso ECHELON. Parla Luigi Ramponi. Anche i politici sapevano, Il mondo, 17.4.1998

[130] Written Question P-0501/98 by Elly Plooij-van Gorsel (ELDR) to the Council (17.1.1998). On 14.5.1997 Jonas Sjöstedt had tabled a question (H-0330/97) on the Council Resolution of 17.1.1995 on the lawful interception of telecommunications, raising the issue of a link with ECHELON. No reply was given to this last part of the question. The questions tabled by Mihail Papayannakis (G-004/98) and Nel van Dijk (H-0035/98) on British espionage activities were answered, on 18.2.1998, to the effect that the activities of intelligence services were exclusively a matter for national authorities and that the Council had no information whatsoever about such activities.

[131] Written Question E-0499/98 to the Council by Elly Plooij-van Gorsel (ELDR) (27.2.1998), Written question E-1775/98 to the Council by Lucio Manisco (GUE/NGL) (8.6.1998), Oral Question H-1086/98 to the Council by Patricia McKenna (16.12.1998), Oral Question H-1172/98 to the Council by Patricia McKenna (13.1.1999), Oral Question H-1172/98 to the Council by Inger Schörling (13.1.1999), Oral Question H-0526/99 to the Council by Pernille Frahm (6.10.1999), Oral Question H-0621/99 to the Council by Lorna Dybkjaer (19.11.1999), etc:

[132] Written Question E-1039/98 by Nel van Dijk (V) (15.5.1998), Written Question E-1306/98 by Cristiana Muscardini (NI) (15.6.1998), Written Question E-1429/98 by Daniela Raschhofer (NI) (25.6.1998), Written Questions E-1987/98 and E-2329/98 by Nikitas Kaklamanis (3.9.1998, 25.9.1998), Written Question E-1776/98 by Lucio Manisco (GUE/NGL), Written Question E-3014/98 by Paul Lannoye (V) (6.11.1998), Oral Question H-0547/99 by Pernille Frahm, Oral Question H-1067/98 by Patricia McKenna (V) (16.12.1998), Oral Question H-1237/98 by Inger Schörling (13.1.1999), Oral Question H-0092/99 by Ionnis Theonas (13.1.1999), Oral Question H-0547/99 by Pernille Frahm (6.10.1999), Oral Question H-0622/99 by Lone Dybkjaer (17.12.1999), etc.

[133] Commissioner Bangemann replying on 25.9.1998, on behalf of the Commission, to Written Question E-1776/98 by Lucio Manisco (GUE/NGL).

[134] Commission President Santer replying on 3.9.1998, on behalf of the Commission, to Written Question E-

14 September 1998, Commissioner Bangemann stated that the Commission had not received from the Member States, members of the public or firms evidence that the interception system existed in the form suggested. 'If the system existed in such a form, that would naturally represent a blatant violation of rights, the individual rights of citizens, and of course an attack on the security of the Member States. That is absolutely clear. The Council, and naturally the Commission and Parliament as well, would have to respond the instant something of that kind was officially confirmed'. The Commission would then 'be using all its powers to persuade the Member States not to obtain information illegally in this way'.[135]

5.10. Parliamentary reports

5.10.1. Reports by the Comité Permanent R, Belgium's monitoring committee

The Belgian monitoring committee, the Comité Permanent R, has already discussed ECHELON in two reports.

The third chapter of its 1999 activity report was devoted to how the Belgian intelligence services are reacting to the possible existence of an ECHELON system of communications surveillance. The 15-page report concludes that both the Belgian intelligence services, the Sûreté de l'Etat and the Service General du Renseignement (SGR), only found out about ECHELON through documents in the public domain.

The second report (rapport complémentaire d'activités 1999) deals with the ECHELON system in much greater detail. It gives a view on the STOA study and devotes one section to explaining the technical and legal background to telecommunications monitoring. It concludes that ECHELON does in fact exist and is also in a position to listen in to all information carried by satellite (approximately 1% of total international telephone communications), in that it searches for keywords, and that its decoding capacity is much greater than the Americans claim. Doubt remains about the accuracy of statements that no industrial espionage is carried out at Menwith Hill. The report makes it clear that it is impossible to ascertain with any certainty what ECHELON does or does not do.

5.10.2. Report by the French National Assembly's Committee on National Defence

The French National Assembly's Committee on National Defence has drawn up a report on surveillance systems[136]. At the meeting held on 28 November 2000 the rapporteur, Arthur Paecht, presented the report's findings to the Temporary Committee.

Following a detailed discussion of a wide variety of aspects, the rapporteur, Arthur Paecht, comes to the conclusion that ECHELON exists and is, in his view, the only known multinational

---

1987/98.

[135] Debates of the European Parliament, sitting of Monday, 14 September 1998, Item 7, Transatlantic relations/ECHELON system.

[136] Rapport d'information déposé en application de l'article 145 du règlement par la commission de la défense nationale et des forces armées, sur les systèmes de surveillance et d'interception électroniques pouvant mettre en cause la sécurité nationale, No 2623 Assemblée nationale, enregistré à la Présidence de l'Assemblée nationale le 11 octobre 2000.

surveillance system. The system's capacities are real but have reached their limits not only because the expenditure can no longer keep pace with the explosion in communications but also because certain targets now know how to protect themselves.

The ECHELON system has moved away from its original goals, which were linked to the Cold War, and this means that it is not impossible that the intelligence gathered may be used for political and industrial purposes against other Nato states.

ECHELON might indeed present a danger to fundamental freedoms and in this context it raises numerous problems that demand appropriate answers. It would be wrong to imagine that the ECHELON member states will give up their activities. On the contrary, there are several indications of a new system being created with new partners as a way of acquiring additional resources to overcome ECHELON's limits.

5.10.3. Report of the Italian Parliament's Committee on Intelligence and Security Services and State Security

In Italy the parliamentary Committee on Intelligence and Security Services drew up a report entitled 'The role of the intelligence and security services in the ECHELON case'[137], which was forwarded to the President of the Italian Parliament on 19 December 2000.

The conclusions concerning the existence of a system named ECHELON are vague. According to the report, 'during the hearings in committee the existence of an integrated interception system of that name, operated by the five signatory states to the UKUSA Agreement (USA, United Kingdom, Australia, New Zealand and Canada) and designed to intercept communications on a worldwide basis was largely ruled out'. Although the existence of closer cooperation among the English-speaking countries was not in doubt, the committee had failed to find evidence that the cooperation was geared to the establishment of an integrated interception system or even a worldwide interception network. The committee felt it was likely that the name ECHELON denoted a stage reached in the development of technology for the interception of satellite communications. The report made explicitly clear that the Italian secret service SISMI had ruled out the existence of an automatic system for the recognition of words used in conversations, so that the targeted interception of conversations containing given keywords was not feasible.

[137] Il ruolo dei servizi di informazione e sicurezza nel caso 'Echelon'.' Relazione del comitato parlamentare per i servizi di informazione e sicurezza e per il segreto di stato. Approvata nella seduta del 29 novembre 2000. Trasmessa alle Presidenze il 19 dicembre 2000.

6. Might there be other global interception systems?

6.1. Requirements of such a system

6.1.1. Technical and geographical requirements

Listening in to international communications transmitted by first-generation satellites requires receiving stations in the Atlantic, the Indian Ocean and the Pacific area. In the case of the newer generation of satellites, which can transmit to sub-regions, further requirements with regard to the geographical position of listening stations would have to be met if all communications via satellite were to be intercepted.

Any other interception system operating on a global scale would be forced to establish its stations outside the territory of the UKUSA states.

6.1.2. Political and economic requirements

The establishment of an interception system of this kind operating on a global scale would, however, also have to make economic and political sense for the operator or operators. The beneficiary or beneficiaries of such a system would have to have global economic, military or other security interests, or at least believe that they were among the world's superpowers. Consequently, we are essentially talking only about China and the G-8 States, excluding the United States and the United Kingdom.

6.2. France

France has its own territories, departments and regional authorities in all three areas listed above.

In the Atlantic, there is St Pierre and Miquelon east of Canada (65º W/47º N), Guadeloupe, north-east of South America (61º W/16º N), and Martinique (60º W/14º N) and French Guyana on the north-east coast of South America (52º W/5º N).

In the Indian Ocean there is Mayotte to the east of southern Africa (45º E/12º S) and Réunion (55º E/20º S) and to the very south the French Southern and Antarctic Territories. In the Pacific there is New Caledonia (165º E/20º S), the Wallis and Futuna Islands (176º W/12º S) and French Polynesia (150º W/16º S).

Very little information is available about possible stations operated by the French intelligence service (DGSE) in these overseas areas. According to reports by French journalists[138], there are stations in Kourou in French Guyana and in Mayotte. No details are available as to the size of the stations, the number of satellite antennae or their size. There are apparently other stations in France at Domme near Bordeaux and at Alluetts-le-Roi near Paris. Vincent Jauvert estimates that there is a total of 30 satellite antennae. The author, Erich Schmidt-Eenboom[139] claims that a station is also operating in New Caledonia and is used by the German Federal Intelligence Service.

Theoretically, since it meets the geographical, technical and financial requirements, France could also operate a global interception system. However, there is insufficient information available in the public domain for your rapporteur to seriously assume that this is the case.

6.3. Russia

The Russian intelligence service FAPSI (Federal Agency of Government Communications and Information, Federalnoye Agentstvo Pravitelstvennoy Svyazi), which is responsible for communications security and SIGINT, operates ground stations in Latvia, Vietnam and Cuba in cooperation with the Russian military intelligence service GRU.

On the basis of the relevant legal provisions, FAPSI's role is to collect political, economic, military and scientific and technological information with a view to fostering economic, military and scientific and technological development[140]. In addition, in 1997 the Director of FAPSI described its primary tasks as the interception of encrypted foreign communications and global interception[141].

In the Atlantic area, the Federation of American Scientists claims that there is a facility at Lourdes in Cuba (82º W/23º N), which is operated jointly with the Cuban intelligence service. With the aid of this station, Russia both gathers strategic intelligence and intercepts military and

[138] *Jean Guisnel*, L'espionnage n'est plus un secret, The Tocqueville Connection, 10.7.1998.
Vincent Jauvert, Espionnage, comment la France écoute le monde, Le Nouvel Observateur, 5.4.2001, No 1900, 14 et seq.
[139] *Erich Schmidt-Eenboom*, in: Streng Geheim, Museumsstiftung Post und Telekommunikationn, Heidelberg (1999), 180.
[140] Russian Federation Federal Law on Foreign Intelligence, adopted by the Duma on 8 December 1995, Sections 5 and 11
[141] Quoted in *Gordon Bennett*, Conflict Studies and Research Centre, The Federal Agency of Government communications and Information, August 2000, http://www.csrc.ac.uk/pdfs/c105.pdf

commercial communications.[142] In the Indian Ocean there are stations in Russia, about which no further information is available. A further station in Skundra in Latvia was closed in 1998[143]. In the Pacific there is apparently a station at Cam Rank Bay in North Vietnam. No detailed information is available about the stations as far as the number and size of the antennae are concerned.

Together with the stations available in Russia itself, global coverage is theoretically possible. However, here too, the information available is insufficient to draw any firm conclusions.

6.4. The other G-8 States and China

Neither the other G-8 States or China have territories or close allies in the parts of the world that would enable them to operate a global interception system.

[142] Quoted in *Gordon Bennett*, Conflict Studies and Research Centre, The Federal Agency of Government Communications and Information, August 2000, http://www.csrc.ac.uk(pdfs/c105.pdf
[143] Homepage of the Federation of American Scientists (FAS), http://www.fas.org

7. Compatibility of an 'ECHELON' type communications interception system with Union law

7.1. Preliminary considerations

The committee's remit includes the specific task of examining the compatibility of an 'ECHELON' type communications interception system with Community law[144]. In particular, it is to examine whether such a system complies with the two data protection Directives 95/46/EC and 97/66/EC, with Article 286 TEC, and Article 8(2) TEU.

This matter has to be considered from two different angles. The first arises from the circumstantial evidence set out in Chapter 5, which indicates that the system known as 'ECHELON' was designed as a communications interception system to provide the US, Canadian, Australian, New Zealand and British secret services with information about events abroad by collecting and evaluating communications data. As such, it is a conventional espionage tool used by foreign intelligence services[145]. Initially, therefore, we will examine the compatibility of such an intelligence system with Union law.

In addition, the STOA report by Duncan Campbell alleges that the system has been misused for purposes of obtaining competitive intelligence, causing serious losses to the industries of European countries. Furthermore, there are statements by the former CIA Director R. James Woolsey, that although the USA was spying on European firms, this was only to restore a level playing field since contracts had only been secured as a result of bribery[146]. If it is true that the system is used to obtain competitive intelligence, the further issue arises of whether this is compatible with Community law. This second aspect will therefore be discussed separately.

7.2. Compatibility of an intelligence system with Union law

7.2.1. Compatibility with EC law

In principle, activities and measures undertaken for the purposes of state security or law enforcement do not fall within the scope of the EC Treaty. As, on the basis of the principle of limited authority, the European Community can only take action where a corresponding competence has been conferred on it, the Community rightly excluded these areas from the scope of application of the data protection directives, which are based on the EC Treaty, and in particular Article 95 (ex-Article 100a) thereof. Directive 59/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data[147] and Directive 97/66/EC concerning the processing of personal data and the protection of privacy in the telecommunications sector[148] do not apply to 'the processing of data[149]/activities[150]

[144] See Chapter 1, 1.3, above.
[145] See Chapter 2 above.
[146] See Chapter 5, 5.6. and 5.8.
[147] OJ L 281 1995, p. 31.
[148] OJ L 24 1998, p. 1.
[149] Art. 3(2), Directive 95/46.
[150] Art. 1(3), Directive 97/66.

concerning public security, defence, state security (including the economic well-being of the state when the activities relate to state security matters) and the activities of the state in areas of criminal law'. Exactly the same wording has been used in the proposal for a directive concerning the processing of personal data and the protection of privacy in the electronic communications sector[151] which is currently before Parliament. The involvement of a Member State in an interception system for the purposes of State security cannot therefore be in breach of the EC's data protection directives.

Similarly, there can be no breach of Article 286 TEC, which extends the scope of the data protection directives to data processing by Community institutions and bodies. The same applies to Regulation 45/2001on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data[152]. This regulation is also applicable only in so far as the bodies are acting within the framework of the EC Treaty[153]. To avoid misunderstandings, it should be clearly emphasised at this point that no sources whatsoever contend that there is any involvement of Community bodies and institutions in a surveillance system and the rapporteur has absolutely no grounds for assuming this to be the case.

7.2.2. Compatibility with other EU law

As far as the areas covered by Title V (common foreign and security policy) and Title VI (police and judicial cooperation in criminal matters) are concerned, there are no data protection provisions comparable to those of the EC directives. The European Parliament has already pointed out on numerous occasions that action is much needed in this area[154].

The protection of the fundamental rights and freedoms of the individual in these spheres is ensured only by Articles 6 and 7, in particular by Article 6(2) TEU, in which the Union undertakes to respect fundamental rights, as guaranteed by the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR) and as they derive from the constitutional traditions common to the Member States. Not only are fundamental rights, and in particular the ECHR, binding on the Member States (see Chapter 8), but the Union is also required to comply with fundamental rights in its legislation and administration. However, since at EU level there are still no regulations concerning the admissibility of the interception of telecommunications for security or intelligence purposes[155], the issue of infringement of Article 6(2) TEU does not yet arise.

---

[151] COM(2000) 385 final, OJ C 365 E/223.

[152] Regulation (EC) No 45/2001, OJ L 8, p.1.

[153] Art. 3(1) and Recital 15 'Where such processing is carried out by Community institutions or bodies in the exercise of activities falling outside the scope of this Regulation, in particular those laid down in Titles V and VI of the Treaty on European Union, the protection of individuals' fundamental rights and freedoms shall be ensured with due regard to Article 6 of the Treaty on European Union.'

[154] See, for example, para 25 of the resolution on the draft action plan of the Council and Commission on how best to implement the provisions of the Treaty of Amsterdam on an area of freedom, security and justice (13844/98 - C4-0692/98 - 98/0923(CNS)), OJ C 219, 30.7.1999, p. 61 et seq.

[155] In the area of telecommunications surveillance there are currently only two EU legislative acts, neither of which covers the question of admissibility:
- Council resolution of 17 January 1995 on the lawful interception of telecommunications (OJ C 329, 4.11.1996), the annex to which sets out the technical requirements relating to the lawful interception of modern telecommunications systems, and
- Council Act of 29 May 2000 establishing, in accordance with Article 34 of the Treaty on European Union, the

7.3. The question of compatibility in the event of misuse of the system for the purposes of gathering competitive intelligence

If a Member State were to promote the use of an interception system, which was also used for industrial espionage, by allowing its own intelligence service to operate such a system or by giving foreign intelligence services access to its territory for this purpose, it would undoubtedly constitute a breach of EC law. Under Article 10 TEC, the Member States are committed to acting in good faith and, in particular, from abstaining from any measure which could jeopardise the attainment of the objectives of the Treaty. Even if the interception of telecommunications is not carried out for the benefit of the domestic industry (which would, in fact, be equivalent in effect to State aid, and thus in breach of Article 87 TEC), but for the benefit of a non-member state, activities of this kind would be fundamentally at odds with the concept of a common market underpinning the EC Treaty, as it would amount to a distortion of competition.

In the opinion of the rapporteur, action of this kind would also be an infringement of the data protection directives for the telecommunications sphere[156], since the question of the applicability of the directive has to be resolved from a functional rather than an organisational point of view. This follows not only from the wording of the regulation as regards its scope, but also from the sense of the law. If intelligence services use their capability to gather competitive intelligence, these activities are not being carried out for the purposes of security or law enforcement but for other purposes and would consequently fall fully within the scope of the directive. Article 5 of the directive requires the Member States to ensure the confidentiality of communications. 'In particular, they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications, by others than users'. Pursuant to Article 14, exceptions may be made only where they are necessary to safeguard national security, defence and law enforcement. As industrial espionage is no justification for an exception, it would, in this case, constitute an infringement of Community law.

7.4. Conclusion

To sum up, it can therefore be said that the current legal position is that in principle an ECHELON type intelligence system is not in breach of Union law because it does not concern the aspects of Union law that would be required for there to be incompatibility. However, this applies only where the system is actually used exclusively for the purposes of state security in the broad sense. On the other hand, were it to be used for other purposes and for industrial espionage directed against foreign firms, this would constitute an infringement of EC law. Were a Member State to be involved in such action, it would be in breach of Community law.

Convention on mutual assistance in criminal matters between the Member States of the European Union (OJ 2000 C 197/1, Art. 17), which regulates the conditions under which mutual assistance in criminal matters with regard to telecommunications interception is possible. These provisions in no way curtail the rights of the subjects of tapping as the Member State in which the subject is to be found has the right to refuse mutual assistance if it is not authorised under national law.

[156] Regulation 97/66 EC, OJ L 24/1998, p.1.

8. The compatibility of communications surveillance by intelligence services with the fundamental right to privacy

8.1. Communications surveillance as a violation of the fundamental right to privacy

Any act involving the interception of communications, and even the recording of data by intelligence services for that purpose[157], represents a serious violation of an individual's privacy. Only in a 'police state' is the unrestricted interception of communications permitted by government authorities. In contrast, in the EU Member States, which are mature democracies, the need for state bodies, and thus also intelligence services, to respect individuals' privacy is unchallenged and is generally enshrined in national constitutions. Privacy thus enjoys special protection: potential violations are authorised only following analysis of the legal considerations and in accordance with the principle of proportionality.

The UKUSA states are also well aware of the problem. However, these states' protection provisions are geared to respect for the privacy of their own inhabitants, so that as a rule European citizens do not benefit from them in any way. For example, the US provisions which lay down the conditions governing electronic surveillance do not set the state's interest in operating a properly functioning intelligence service against the interests of effective, general protection fundamental rights, but rather against the need to protect the privacy of 'US persons'[158].

8.2. The protection of privacy under international agreements

Many agreements under international law specify respect for privacy as a fundamental right[159]. At world level, particular mention should be made of the International Covenant on Civil and Political Rights[160], which was adopted by the UN in 1966. Article 17 of the Covenant guarantees the protection of privacy. In connection with complaints submitted by other states, all the UKUSA states have complied with the decisions taken by the Human Rights Committee set up

[157] German Federal Constitutional Court (FCC), 1 BVR 226/94 of 14 July 1999, Rz 187: 'The recording of data already represents a violation of that right in so far as it makes the content of the communications available to the Federal Intelligence Service and forms the basis of the ensuing analysis using search terms'.
[158] Compare the report submitted to the US Congress in late February 2000, 'Legal Standards for the Intelligence Community in Conducting Electronic Surveillance', http://www.fas.org/irp/nsa/standards.html, which refers to the Foreign Intelligence Surveillance Act (FISA), printed in Title 50, Chapter 36, USC, § 1801 et seq, and Executive Order No 12333, 3 CFR 200 (1982), printed in Title 50, Chapter 15, USC, § 401 et seq, http://www4.law.cornell.edu/uscode750/index.html.
[159] Article 12 of the Universal Declaration of Human Rights; Article 17 of the UN Covenant on Civil and Political Rights; Article 7 of the EU Charter of Fundamental Rights; Article 8 of the ECHR; Recommendation of the OECD Council on guidelines for the security of information systems, adopted on 26/27 November 1993, C(1992) 188/final; Article 7 of the Council of Europe Convention on the Protection of Persons with regard to the automatic processing of personal data; compare the study commissioned by STOA entitled 'Development of Surveillance Technology and Risk of Abuse of Economic Information; Part. 4/5: the legality of the interception of electronic communications: a concise survey of the principal legal issues and instruments under international, European and national law (Chris Elliot), October 1999, 2.
[160] Adopted by the UN General Assembly on 16 December 1966.

pursuant to Article 41 of the Covenant to rule on breaches of the Covenant under international law. The Optional Protocol[161], which extends the powers of the Human Rights Committee to cover complaints submitted by private individuals, has not been signed by the USA, however, so that such individuals cannot appeal to the Human Rights Committee in the event of the violation of the Covenant by the USA.

At EU level, efforts have been made to establish specifically European arrangements for the protection of fundamental rights through the drafting of a Charter of Fundamental Rights of the EU. Article 7 of the Charter, entitled 'Respect for private and family life', even lays down explicitly in law the right to respect for communications[162]. In addition, Article 8 lays down in law the fundamental right to the 'protection of personal data'. This would have protected individuals in those cases involving the (computerised or non-computerised) processing of their data, something which generally occurs when voice communications are intercepted and invariably does when other forms of communication are intercepted.

The Charter has not yet been incorporated into the Treaty. It is binding, therefore, only on the three institutions which pledged to comply with it in the Formal Declaration adopted during the Nice European Council: the Council, the Commission and the European Parliament. As far as your rapporteur is aware, they are not involved in any secret service activities. Even when the Charter acquires full legal force through its incorporation into the Treaty, due account will have to be taken of its limited scope. Pursuant to Article 51, the Charter applies to 'the institutions and bodies of the Union … and to the Member State only when they are implementing Union law'. Accordingly, the Charter would at best take effect via the ban on state aid schemes which run counter to the principles of competition (see Chapter 7, 7.3.).

The only effective international instrument for the comprehensive protection of privacy is the ECHR.

8.3. The rules laid down in the (ECHR)

8.3.1. The importance of the ECHR in the EU

The protection of fundamental rights provided by the ECHR is particularly important in that the Convention has been ratified by all the EU Member States, thereby creating a uniform level of protection in Europe. The contracting parties have given an undertaking under international law to guarantee the rights enshrined in the ECHR and have declared that they will comply with the judgments of the European Court of Human Rights in Strasbourg. The relevant national legal provisions can thus be reviewed by the European Court of Human Rights as to their conformity with the ECHR and, in the event of a breach of human rights, a judgment may be handed down against the contracting party concerned and it may be required to pay compensation. The ECHR has gained further in importance by being repeatedly invoked by the CJEC, alongside the general legal principles adhered to by the Member States, when that body takes decisions in cases involving legal reviews. Moreover, following the adoption of the Treaty of Amsterdam Article 6(2) of the Treaty on European Union commits the EU to respecting fundamental rights as enshrined in the ECHR.

[161] Optional Protocol to the International Covenant on Civil and Political Rights, adopted by the UN General Assembly on 16 December 1966.
[162] 'Everyone has the right to respect for his or her private family life, home and communications.'

8.3.2. The geographical and personal scope of the protection provided under the ECHR

The rights enshrined in the ECHR represent generally recognised human rights and are thus not linked to nationality. They must be granted to all persons covered by the jurisdiction of the contracting parties. In other words, the human rights in question must at all events be guaranteed throughout the territory of the contracting parties, so that local exceptions would represent a breach of the Convention. In addition, however, they are also valid outside the territory of the contracting parties, provided that state authority is exercised in such places. The rights guaranteed by the ECHR vis-à-vis a contracting state are thus also enjoyed by persons outside the territory of that state if those persons suffer interference in the exercise of their right to privacy[163].

The latter point is particularly important here, since a specific characteristic of the issue of fundamental rights in the area of telecommunications surveillance is the fact that there may be a substantial geographical distance between the state responsible for the surveillance, the person under surveillance and the location in which interception is actually carried out. This applies in particular to international communications, but may also apply to national communications if information is transmitted via connections situated abroad. Indeed, this is typical of interceptions carried out by foreign intelligence services. It is also possible that information obtained by an intelligence service by means of surveillance will be passed on to other states.

8.3.3. The admissibility of telecommunications surveillance pursuant to Article 8 of the ECHR

Pursuant to Article 8(1) of the ECHR, 'everyone has the right to respect for his private and family life, his home and his correspondence'. No explicit reference is made to the protection of telephony or telecommunications, but, under the terms of the case law of the European Court of Human Rights, they are protected by the provisions of Article 8, since they are covered by the concepts of 'private life' and 'correspondence'[164]. The scope of the protection of this fundamental right covers not only the substance of the communication, but also the act of recording external data. In other words, even if the intelligence service merely records data such as the time and duration of calls and the numbers dialled, this represents a violation of privacy[165].

Pursuant to Article 8(2) of the ECHR, exercise of this fundamental right is not unrestricted. Interference in the exercise of the fundamental right to privacy may be admissible if there is a legal basis under national law[166]. The law must be generally accessible and its consequences must be foreseeable[167].

---

[163] Judgment of the European Court of Human Rights, Loizidou/Turkey, 23.3.1995, line 62, with further references: '… the concept of 'jurisdiction' under this provision is not restricted to the national territory of the High Contracting Parties […] responsibility can be involved because of acts of their authorities, whether performed within or outside national boundaries, which produce effects outside their own territory', with reference to the European Court of Human Rights, Drozd and Janousek, 26.6.1992, line 91. See also the comprehensive details in *Francis G. Jacobs, Robin C. A. White*, The European Convention on Human Rights, Clarendon Press (1996), pp. 21 et seq, *Jochen Abr. Frowein, Wolfgang Peukert*, European Convention on Human Rights, N.P. Engel Verlag (1996), Rz 4 et seq.

[164] See European Court of Human Rights, Klass et al, 6.9.1978, line 41.

[165] See European Court of Human Rights, Malone, 2.8.1984, line 83 et seq; also B. Davy/U.Davy, Aspects of state information collection and Article 8 of the ECHR, JBl 1985, 656.

[166] Under the case law of the European Court of Human Rights (in particular Sunday Times, 26.4.1979, line 47 et

In that connection, the Member States are not free to interfere in the exercise of this fundamental right as they see fit. They may do so only for the purposes listed in the second paragraph of Article 8 of the ECHR, in particular in the interests of national security, public safety or the economic well-being of the country[168]. However, this does not justify industrial espionage, since it only covers forms of interference 'necessary in a democratic society'. In connection with any instance of interference, the least invasive means appropriate must be employed to achieve the objective; in addition, adequate guarantees must be laid down to prevent misuse of this power.

8.3.4. The significance of Article 8 of the ECHR for the activities of intelligence services

These general principles have the following implications for the organisation of the work of intelligence services in a manner consistent with this basic right: if, for the purpose of safeguarding national security, there seems to be a need to authorise intelligence services to record the substance of telecommunications, or at least external data relating to the connections in question, this power must be established in national law and the relevant provisions must be generally accessible. The consequences for individuals must be foreseeable, but due account must be taken of the particular requirements in the sphere of national security. Accordingly, in a ruling on the conformity with Article 8 of secret checks on employees in areas relating to national security, the European Court of Human Rights noted that in this special case the arrangements governing the foreseeability requirement must differ from those in other areas[169]. In this context as well, however, it stipulated that the law must at all events state under what circumstances and subject to what conditions the state may carry out secret, and thus potentially dangerous, interference in the exercise of the right to privacy[170].

In connection with the organisation of the activities of intelligence services in a manner consistent with human rights, due account must be taken of the fact that, although national security can be invoked to justify an invasion of privacy, the principle of proportionality, as defined in Article 8(2) of the ECHR, also applies: national security represents valid grounds only in cases where action to protect it is necessary in a democratic society. In that connection, the European Court of Human Rights has clearly stated that the interest of the state in protecting its national security must be weighed up against the seriousness of the invasion of an individual's privacy[171]. Invasions of privacy may not be restricted to the absolute minimum, but mere usefulness or desirability is not sufficient justification[172]. The view that the interception of all

---

seq, Silver et al, 25.3.1983, line 85 et seq, the term 'the law' in Article 8(2) embraces not only laws in the formal sense, but also legal provisions below the level of a law and, in certain circumstances, even unwritten law. It is essential, however, that it is clear to the legal subject under what circumstances interference is possible. For more details see *Wolfgang Wesseley*, Telecommunications Privacy – an unknown basic right?, ÖJZ 1999, pp. 491 et seq, 495.

[167] Silver et al, 25.3.1983, line 87 et seq.

[168] The justification of 'economic well-being' was accepted by the European Court of Human Rights in a case involving the transmission of medical data relevant to the award of public compensation, M.S./Sweden, 27.8.1997, line 38; and in a case involving the expulsion from the Netherlands of a person who had been living on welfare payments after the grounds for the award of a residence permit had ceased to apply, Ciliz/Netherlands, 11.7.2000, line 65.

[169] European Court of Human Rights, Leander, 26.3.1987, line 51.

[170] European Court of Human Rights, Malone, 2.8.1984, line 67.

[171] European Court of Human Rights, Leander, 26.3.1987, line 59, Sunday Times, 26.4.1979, line 46 et seq.

[172] European Court of Human Rights, Silver et al, 24.10.1983, line 97.

telecommunications, even if permissible under national law, represents the best form of protection against organised crime would amount to a breach of Article 8 of the ECHR.

In addition, given the specific nature of the activities conducted by intelligence services, activities which demand secrecy and, therefore, a particularly careful weighing-up of interests, provision must be made for more stringent monitoring arrangements. The European Court of Human Rights has explicitly drawn attention to the fact that a secret surveillance system operated for the purpose of protecting national security carries with it the risk that, under the pretext of defending democracy, it may undermine or even destroy the democratic system, so that more appropriate and more effective guarantees are needed to prevent such misuse of powers[173]. Accordingly, the legally authorised activities of intelligence services are only consistent with fundamental rights if the ECHR contracting party has established adequate systems of checks and other guarantees to prevent the misuse of powers.

In connection with the activities of Sweden's intelligence services, the European Court of Human Rights emphasised the fact that it attaches particular importance to the presence of MPs in police supervisory bodies and to supervision by the Minister of Justice, the parliamentary Ombudsman and the parliamentary Committee on Legal Affairs. Against this background, it must be regarded as unsatisfactory that France, Greece, Ireland, Luxembourg and Spain have no parliamentary committee with responsibility for monitoring the secret services[174] and have made no move to set up a supervisory system similar to the office of parliamentary Ombudsman pioneered by the Nordic states[175]. Your rapporteur therefore welcomes the efforts made by the French National Assembly Committee on National Defence to set up a monitoring committee[176], particularly as France has exceptional intelligence capabilities, in both technical and geographical terms.

8.4. The requirement to monitor closely the activities of other countries' intelligence services

8.4.1. Inadmissibility of moves to circumvent Article 8 of the ECHR through the use of other countries' intelligence services

As outlined in detail above, the contracting parties must comply with a set of conditions in order to demonstrate that the activities of their intelligence services are compatible with Article 8 of the ECHR. It is quite obvious that intelligence services cannot be allowed to circumvent these requirements by employing assistance from other intelligence services subject to less stringent rules. Otherwise, the principle of legality, with its twin components of accessibility and foreseeability, would become a dead letter and the case law of the European Court of Human Rights would be deprived of its substance.

[173] European Court of Human Rights, Leander, 26.3.1987, line 60.
[174] Your rapporteur is aware that neither Luxembourg nor Ireland has a foreign intelligence service and does not carry out SIGINT operations. The need for a specific supervisory body relates here only to domestic intelligence activities.
[175] For details of the situation regarding the supervision of intelligence services in the Member States, see Chapter 9.
[176] Bill entitled 'Proposition de loi tendant à la création de délégations parlementaires pour le renseignement', and the related report by *Arthur Paecht*, Rapport fait au nom de la Commission de la défense nationale et des forces armées sur la proposition de loi (N° 1497) de M. Paul Quilès et plusieurs de ses collègues tendant à la création d'une délégation parlementaire pour les affaires de renseignement, enregistré à la Présidence de l'assemblée nationale le 23. novembre 1999

The first implication of this is that exchanges of data between intelligence services are permissible only on a restricted basis. An intelligence service may seek from one of its counterparts only data obtained in a manner consistent with the conditions laid down in its own national law. The geographical scope for action laid down by law in respect of the intelligence service concerned may not be extended by means of agreements with other services. By the same token, it may carry out operations on behalf of another country's intelligence service, in accordance with the latter's instructions, only if it is satisfied that the operations are consistent with the national law of its own country. Even if the information is intended for another country, this in no way alters the fact that an invasion of privacy which could not be foreseen by the legal subject concerned constitutes a violation of fundamental rights.

The second implication is that states which are ECHR contracting parties may not allow other countries' intelligence services to carry out operations on their territory if they have reason to believe that those operations are not consistent with the conditions laid down by the ECHR[177].

8.4.2. Implications of allowing non-European intelligence services to carry out operations on the territory of Member States which are ECHR contracting parties

8.4.2.1. The relevant case law of the European Court of Human Rights

By ratifying the ECHR the contracting parties undertook to subject the exercise of their sovereignty to a review of its consistency with fundamental rights. They cannot seek to circumvent this requirement by foregoing the exercise of that sovereignty. These states remain responsible for their territory and thus have an obligation to European legal subjects if the exercise of sovereignty is usurped by the activities of the intelligence services of another state. The established case law of the European Court of Human Rights now emphasises that the contracting parties have a duty to take positive measures to protect privacy, in order to ensure that private individuals (!) do not violate Article 8 of the ECHR. In other words, they must take action even at a horizontal level, where private individuals are not confronted with the actions of the state, but rather of other private individuals[178]. If a state allows another country's intelligence service to work on its territory, the protection requirement is much greater, because in that case another authority is exercising its sovereignty. The only logical conclusion is that states must carry out checks to ensure that the activities of intelligence services on their territory do not represent a violation of human rights.

8.4.2.2. Implications for stations

In Bad Aibling in Germany an area of land has been declared US territory for the sole purpose of housing a satellite receiving facility. In Menwith Hill in the United Kingdom authorisation has been given for the shared use of land for the same purpose. If, in these stations, a US intelligence service were to engage in the interception of non-military communications conducted by private individuals or firms from an ECHR contracting party, supervisory requirements would come into play under the ECHR. In practical terms, as ECHR contracting parties Germany and the United

[177] See also *Dimitri Yernault*, 'ECHELON and Europe. The protection of privacy against communications espionage', Journal of the Courts, European Law, 2000, 187 et seq.

[178] European Court of Human Rights, Abdulaziz, Cabales and Balkandali, 28.5.1985, line 67; X and Y/Netherlands, 26.3.1985, line 23; Gaskin v United Kingdom, 7.7.1989, line 38; Powell and Rayner, 21.2.1990, line 41.

Kingdom are required to establish that the activities of the American intelligence services do not represent a violation of fundamental rights. This is all the more relevant because representatives of NGOs and the press have repeatedly expressed concerns regarding the activities of the US National Security Agency (NSA).

8.4.2.3. Implications for interception carried out on behalf of third parties

According to information available to the committee, in Morwenstow in the United Kingdom GCHQ, working in cooperation with the NSA and in strict accordance with the latter's instructions, intercepts civilian communications and passes on the recordings to the USA as raw intelligence material. The requirement to check that interception operations are consistent with fundamental rights also applies to work carried out on behalf of third parties.

8.4.2.4. Particular duty of care in connection with third states

In the case of operations involving two ECHR contracting parties, both can assume, up to a certain point, that the other is complying with the ECHR. At all events, this applies until evidence emerges that an ECHR contracting party is violating the Convention on a systematic, long-term basis. Things are very different, however, in the case of the USA: it is not an ECHR contracting party and it has not made its intelligence operations subject to a similar supervisory system. There are very precise rules governing the activities of its intelligence services, in so far as those activities concern US citizens or persons legally present on US territory. However, other rules apply to the activities of the NSA abroad, and many of the relevant rules are classified and thus inaccessible to the public. A further fact gives greater cause for concern, namely that although the US intelligence service is subject to monitoring by the relevant House of Representatives and Senate committees, these committees show little interest in the activities of the NSA abroad.

There would seem to be good reason, therefore, to call on Germany and the United Kingdom to take their obligations under the ECHR seriously and to make the authorisation of further intelligence activities by the NSA on their territory contingent on compliance with the ECHR. In this connection, three main factors must be considered.

1. Under the terms of the ECHR, interference in the exercise of the right to privacy may only be carried out on the basis of legal rules which are generally accessible and whose implications for individuals are foreseeable. This requirement can be met only if the USA discloses to the public in Europe how and under what circumstances intelligence-gathering is carried out. If incompatibilities with the ECHR emerge, US rules must be brought into line with the level of protection provided in Europe.

2. Under the terms of the ECHR, interference in the exercise of the right to privacy must be proportional and, in addition, the least invasive methods must be chosen. As far as European citizens are concerned, an operation constituting interference carried out by a European intelligence service must be regarded as less serious than one conducted by a US intelligence service, since only in the first instance is legal redress available in the national

courts[179]. Operations constituting interference must therefore be carried out, as far as possible, by the German or UK authorities, particularly when investigations are being conducted for law enforcement purposes . The US authorities have repeatedly tried to justify the interception of telecommunications by accusing the European authorities of corruption and taking bribes[180]. It should be pointed out to the Americans that all EU Member States have properly functioning criminal justice systems. If there is evidence that crimes have been committed, the USA must leave the task of law enforcement to the host countries. If there is no such evidence, surveillance must be regarded as unproportional, a violation of human rights and thus inadmissible. In other words, compliance with the ECHR can be guaranteed only if the USA restricts itself to surveillance measures conducted for the purpose of safeguarding its national security, but not for law enforcement purposes.

3. As already outlined above, in its case law the European Court of Human Rights has stipulated that compliance with fundamental rights is contingent on the existence of adequate monitoring systems and guarantees against abuse. This implies that US telecommunications surveillance operations carried out on European territory are consistent with human rights only if the USA introduces appropriate, effective checks on such operations carried out for the purpose of safeguarding its national security or if the NSA makes its operations on European territory subject to the authority of the control bodies set up by the host state, i.e. Germany or the United Kingdom.

The conformity of US telecommunications interception operations with the ECHR can only be guaranteed and the uniform level of protection provided in Europe by the ECHR can only be maintained if the requirements set out in the three points above are met.

[179] This is also necessary for compliance with Article 13 of the ECHR, which grants the person whose privacy has been invaded the right to submit a complaint to national courts.
[180] *James Woolsey* (former CIA Director), Why America Spies on its Allies, The Wall Street Journal Europe, 22 March 2000, 31, and Remarks at the Foreign Press Centre, transcript, 7 March 2000, http://cryptome.org/echelon-cia.htm.

9. Are EU citizens adequately protected against the activities of intelligence services?

9.1. Protection against the activities of intelligence services: a task for the national parliaments

Although the activities of intelligence services may be covered by the CFSP in future, as yet no relevant rules have been drawn up at EU level[181], so that any arrangements to protect citizens against the activities of intelligence services can only be made under national legal systems.

In this connection, the national parliaments have a dual role to play: as legislators, they take decisions on the nature and powers of the intelligence services and the arrangements for monitoring their activities. As outlined in detail in the previous chapter, when dealing with the issue of the admissibility of telecommunications surveillance, the national parliaments must work on the basis of the restrictions laid down in Article 8 of the ECHR, i.e. the relevant legal rules must be necessary and proportional and their implications for individuals must be foreseeable. In addition, adequate and effective monitoring arrangements must be introduced commensurate with the powers of the intelligence agencies.

Moreover, in most states the national parliament plays an active role as the monitoring authority, given that, alongside the adoption of legislation, scrutiny of the executive, and thus also the intelligence services, is the second time-honoured function of a parliament. However, the Member State parliaments carry out this task in a very wide variety of differing ways, often on the basis of cooperation between parliamentary and non-parliamentary bodies.

9.2. The powers enjoyed by national authorities to carry out surveillance measures

As a rule, the state may carry out surveillance measures for the purposes of enforcing the law, maintaining domestic order and safeguarding national security (vis-à-vis foreign intervention)[182].

In all Member States, the principle of telecommunications secrecy may be breached for law enforcement purposes, provided that there is sufficient evidence that a crime (possibly one perpetrated under particularly aggravating circumstances) has been committed by a specific person. In view of the seriousness of the interference in the exercise of the right to privacy, a warrant is generally required for such an action[183] it lays down precise details concerning the permissible duration of the surveillance, the relevant supervisory measures and the deletion of the collected data.

For the purposes of guaranteeing national security and order, the state's right to obtain information is extended beyond the scope of individual investigations prompted by firm

[181] See Chapter 7.
[182] Article 8(2) of the ECHR lays down these issues as grounds justifying interference in an individual's exercise of the right to privacy. See Chapter 8, 8.3.2. above.
[183] British law is an exception, giving the Home Secretary the power to issue authorisations (Regulation of Investigatory Powers Act 2000, Section 5(1) and (3)(b)).

evidence that a crime has been committed. National law authorises the state to carry out additional measures to secure information about specific persons or groups with a view to the early detection of extremist or subversive movements, terrorism and organised crime. The relevant data is collected and analysed by specific domestic intelligence services.

Finally, a substantial proportion of surveillance measures are carried out for the purposes of safeguarding state security. As a rule, responsibility for processing, analysing and presenting relevant information about foreign individuals or countries lies with the state's own foreign intelligence service[184]. In general the surveillance targets are not specific persons, but rather set areas or radio frequencies. Depending on the resources and legal powers of the foreign intelligence service concerned, surveillance operations may cover a wide spectrum, ranging from purely military surveillance of short-wave radio transmissions to the surveillance of all foreign telecommunications links. In some Member States the surveillance of telecommunications for purely intelligence purposes is simply prohibited[185], in other Member States – in some cases subject to authorisation by an independent commission[186] - it is carried out on the basis of a ministerial order[187], possibly even without restriction in the case of some communication media[188]. The relatively broad powers enjoyed by some foreign intelligence services can be explained by the fact that their operations are targeted on the surveillance of foreign communications and thus only concern a small proportion of their own legal subjects, hence the substantially concern regarding lesser degree of misuse of their powers.

9.3. Monitoring of intelligence services

Effective and comprehensive monitoring is particularly important for two reasons: firstly, because intelligence services work in secret and on a long-term basis, so that the persons concerned often learn that they were surveillance targets only long after the event or, depending on the legal situation, not at all; and, secondly, because surveillance measures often target broad, vaguely defined groups of persons, so that the state can very quickly obtain a very large volume of personal data.

Irrespective of the form they take, all monitoring bodies naturally face the same problem: given the very nature of secret services, it is often extremely difficult to determine whether all the requisite information has in fact been provided, or whether some details are being held back. The relevant rules must therefore be framed all the more carefully. As a matter of principle, the effectiveness of the monitoring can be said to be high, and far-reaching guarantees that the interference is consistent with the law can be said to exist, if the power to order telecommunications surveillance is reserved for the highest administrative authorities, if the surveillance can be implemented only on the basis of a warrant issued by a judge and if an independent body scrutinises the performance of the surveillance measures. In addition, on

[184] For comprehensive details of the activities of foreign intelligence services, see Chapter 2.
[185] For example, in Austria and Belgium.
[186] For example, in Germany, law on the restriction of post and telecommunications secrecy (Law on Article 10 of the Basic Law). Pursuant to paragraph 9, except in cases where there is a risk that delay would frustrate the operation, the commission must be informed before the surveillance is carried out..
[187] For example in the United Kingdom (Regulation of Investigatory Powers Act, Section 1), and in France for cable communications (Law 91/646 of 10 July 1991 – loi relative au secret des correspondances émises par la voie de télécommunications).
[188] For example cable communications in France (Article 20 of Law 91/646 of 10 July 1991 - loi relative au secret des correspondances émises par la voie de télécommunications).

democratic and constitutional grounds it is desirable that the work of the intelligence service as a whole should be subject to monitoring by a parliamentary body, in accordance with the principle of the division of powers.

In Germany, these conditions have largely been met. Telecommunications surveillance measures at national level are ordered by the responsible federal minister. Unless there is a risk that further delay may frustrate the operation, prior to the implementation of surveillance measures an independent commission not bound by government instructions (G10 Commission[189]) must be notified so that it can rule on the need for and the admissibility of the proposed measure. In those cases in which the German Federal Intelligence Service, FIS, can be authorised to carry out surveillance of non-cable telecommunications traffic with the aid of filtering on the basis of search terms, the Commission rules on the admissibility of the search terms as well. The G10 Commission is also responsible for checking that the persons under surveillance are notified, as required by the law, and that the FIS destroys the collected data.

Alongside this, there is a parliamentary monitoring body (PMB)[190], which comprises nine Members of the Bundestag and scrutinises the activities of all three German intelligence services. The PMB has the right to inspect documents, to take evidence from intelligence service staff, to visit the premises of the services and to have information notified to it; this last right can be denied only on compelling grounds concerning access to information, if it is necessary to protect the right of privacy of third parties, or if the core area of government responsibility is concerned. The proceedings of the PMB are secret and its members are required to maintain confidentiality even after they have left office. At the half-way point and at the end of the parliamentary term, the PMB submits to the German Bundestag a report on its monitoring activities.

It must be said, however, that comprehensive, monitoring of intelligence services is the exception in the Member States.

In France[191], for example, only those surveillance measures entailing the tapping of a cable require the authorisation of the Prime Minister. Only measures of that kind are subject to monitoring by the Commission set up for that purpose (National Commission for the Monitoring of Security-related Interceptions), whose members include an MP and a Senator. Applications for authorisation to carry out an interception operation are submitted by a minister or his or her representative to the chairman of the Commission, who, if the lawfulness of the proposed operation is in doubt, may convene a meeting of the Commission, which issues recommendations and, if there are grounds for suspecting a breach of the criminal law, informs the state prosecutor's office. Measures carried out in defence of national interests which entail the interception of radio transmissions, and thus also satellite communications, are not subject to any restrictions, including monitoring by a commission.

Moreover, the work of the French intelligence services is not subject to scrutiny by a parliamentary monitoring committee; however, moves are afoot to set up such a committee. The

[189] For full details see 'The Parliamentary Supervision of the Intelligence Services in Germany, as at 9.9.2000', published by the German Bundestag, Secretariat of the Parliamentary Control Body.
[190] Law on the supervision of federal intelligence activities (PKGrG) of 17 June 1999, BGBl I 1334 idgF.
[191] Law 91-646 of 10 July 1991; loi relative au secret des correspondances émises par la voie de télécommunications.

Defence Committee of the National Assembly has already approved such a proposal[192], but no discussion of that proposal has yet taken place in plenary.

In the United Kingdom, every communications surveillance measure carried out on British soil requires the authorisation of the Home Secretary. However, the wording of the law does not make it clear whether the non-targeted interception of communications, communications which are then checked using keywords, would also be covered by the concept of 'interception' as defined in the Regulation of Investigatory Powers Act 2000 (RIP) if the intercepted communications were not analysed on British soil, but merely transmitted abroad as 'raw material'. Checks on compliance with the provisions of the RIP are carried out on an ex-post facto basis by Commissioners – sitting or retired senior judges appointed by the Prime Minister. The Interception Commissioner monitors the granting of interception authorisations and supports investigations into complaints concerning interception measures. The Intelligence Service Commissioner monitors the authorisations granted for the activities of the intelligence and security services and supports investigations into complaints concerning those services. The Investigatory Powers Tribunal, which is chaired by a senior judge, investigates all complaints concerning interception measures and the activities of the services referred to above.

Parliamentary scrutiny is carried out by the Intelligence and Security Committee (ISC)[193], which monitors the activities of all three civilian intelligence services (MI5, MI6 and GCHQ). In particular, it is responsible for scrutinising the expenditure and administration and monitoring the activities of the security service, the intelligence service and GCHQ. The committee comprises nine members drawn from the two Houses of Parliament; ministers may not be members. Unlike the monitoring committees set up by other states, which are generally elected by the national parliament or appointed by the Speaker of that parliament, they are appointed by the Prime Minister after consulting the Leader of the Opposition.

These examples already demonstrate clearly that the level of protection varies very substantially. As far as parliamentary scrutiny is concerned, your rapporteur would like to point out that the existence of a monitoring committee responsible for scrutinising the activities of intelligence services is very important: in contrast to the normal parliamentary committees, they have the advantage of enjoying a higher degree of trust among the intelligence services, given that their members are bound by the confidentiality rule and committee meetings are held in camera. In addition, with a view to the performance of their special task they are endowed with special rights vital to the monitoring of activities in the intelligence sector.

Your rapporteur is pleased to report that most of the EU Member States have set up a separate parliamentary monitoring committee to scrutinise the activities of the intelligence services. In Belgium[194], Denmark[195], Germany[196], Italy[197], the Netherlands[198] and Portugal[199], there is a

[192] See the Bill entitled 'Proposition de loi tendant á la création de délégations parlementaires pour le renseignement', and the related report by *Arthur Paecht*, Rapport fait au nom de la Commission de la défense nationale et des forces armées sur la proposition de loi (N° 1497) de M. Paul Quilès et plusieurs de ses collègues tendant à la création d'une délégation parlementaire pour les affaires de renseignement, enregistré à la Présidence de L'Assemblée nationale le 23 novembre 1999

[193] Intelligence Services Act 1994, Section 10.

[194] Comité permanent de côntrole des services de renseignements et de sécurité, Comité permanent R, Loi du 18 juillet 1991 / IV, organique du contrôle des services de police et de renseignements.

[195] Udvalget vedrørende efterretningstjenesterne, Lov om etablering af et udvalg om forsvarets og politiets efterretningsjenester, lov 378 af 6.7.88.

parliamentary monitoring committee responsible for scrutinising both the military and civilian intelligence service. In the United Kingdom[200] the special monitoring committee scrutinises only the admittedly much more significant activities of the civilian intelligence services; the military intelligence service is monitored by the normal defence committee. In Austria[201] the two arms of the intelligence service are dealt with by two separate monitoring committees, which are, however, organised in the same way and endowed with the same rights. In the Nordic states Finland[202] and Sweden[203] parliamentary scrutiny is carried out by Ombudsmen, who are independent and elected by parliament. France, Greece, Ireland, Luxembourg and Spain have no special parliamentary committees; in these countries, monitoring tasks are carried out by the standing committees as part of their general parliamentary work.

9.4. Assessment of the situation for European citizens

The situation for European citizens in Europe is unsatisfactory. The powers of national intelligence services in the sphere of telecommunications surveillance differ very substantially in scope, and the same applies to the powers of the monitoring committees. Not all those Member States which operate an intelligence service have also set up independent parliamentary monitoring bodies endowed with the appropriate supervisory powers. A uniform level of protection is still a distant objective.

From a European point of view, this is all the more regrettable, because this state of affairs does not primarily affect the citizens of the Member States concerned, who can influence the level of protection by means of their voting behaviour in elections. The adverse impact is felt above all by nationals of other states, since foreign intelligence services, by their very nature, carry out their work abroad. Individuals are essentially at the mercy of foreign systems, and here the need for protection is greater still. It must also be borne in mind that, by virtue of the specific nature of intelligence services, EU citizens may be affected by the activities of several such services at the same time. In this context, a uniform level of protection consistent with democratic principles would be desirable. Consideration should also be given to the issue of whether data protection provisions in this sphere would be workable at EU level.

---

[196] Das parlamentarische Kontrollgremium (PKGr), Gesetz über die Kontrolle nacrhichtendienstlicher Tätigkeit des Bundes (PKGrG) vom 17 Juni 1999 BGB1 I 1334 idgF.

[197] Comitato parlamentare, L. 24 ottobre 1977, n. 801, art. 11, Istituzione e ordinamento de servizi per le informazioni e la sicurezza e disciplina del segreto di Stato.

[198] Tweede-Kamercommissie voor de Inlichtingen-en Veiligheidsdiensten, 17. Reglement van order van de Tweede Kamer der Staten-General, Art. 22.

[199] Conselho de Fiscalização dos Serviços de Informações (CFSI), Law 30/84 of 5.9.1984, amended by Law 4/95 of 21.2.1995, Law 15/96 of 30.4.1996 and Law 75-A/97 of 22.7.1997.

[200] Intelligence and Security Committee (ISC), Intelligence Services Act 1994, Section 10.

[201] Standing Subcommittee of the National Defence Committee responsible for monitoring intelligence measures to safeguard military security and the Standing Subcommittee of the Committee on Internal Affairs responsible for monitoring measures to protect constitutional bodies and their ability to act, Article 52a B-VG, §§ 32b et seq., Law on the Rules of Procedure, 1975.

[202] Ombudsman, legal basis for supervision of the police (SUPO): Poliisilaki 493/1995 § 33 and Laki pakkokeinolain 5 a luvun muuttamisesta 366/1999 § 15, for the military: Poliisilaki 493/1995 § 33 and Laki poliisin tehtävien suorittamisesta puolustusvoimissa 1251/1995 § 5.

[203] Rikspolisstyrelsens ledning, Förordning (1998: 773) med instruktion för Rikspolisstyrelsen (Regulation (1989: 773) on the national police authority).

Moreover, the issue of the protection of European citizens will be placed in an entirely new context when, under a common security policy, the first moves are made towards cooperation among the Member States' intelligence services. Citizens will then look to the European institutions to adopt adequate protection provisions. The European Parliament, as an advocate of constitutional principles, will then have the task of lobbying for the powers it needs, as a democratically elected body, to carry out appropriate monitoring. In this connection, the European Parliament will also be required to establish conditions under which the confidential processing of sensitive data of this kind and other secret documents by a special committee whose members are bound by a duty of discretion can be guaranteed. Only once these conditions have been met will it be realistic, and, with a view to effective cooperation among intelligence services – the *sine qua non* of a serious common security policy – responsible, to press for these monitoring rights.

10. Protection against industrial espionage

10.1. Firms as espionage targets

The information held by firms falls into three categories as far as the need for secrecy is concerned. Firstly, there is information which is deliberately **disseminated as widely as possible**. This includes technical information about a firm's products (e.g. specifications, prices, etc.) and promotional information which has a bearing on a firm's image.

Secondly, there is information which is **neither protected nor actively disseminated**, because it has no bearing on a firm's competitive position. Examples includes the date of the works outing, the menu in the works canteen or the make of fax machine used by a firm.

Finally, there is information which is **protected against third parties**. The information is protected against competitors, but also, if a firm intends to break the law (tax provisions, embargo rules, etc.), against the state. There are various degrees of protection, culminating in strict secrecy, e.g. in the case of research findings prior to the registration of a patent or armaments production[204].

In the case under discussion here, espionage involves obtaining information kept secret by a firm. If the assailant is a rival firm, the term used is **competitive intelligence**. If the assailant is a state intelligence service, the relevant term is **industrial espionage**.

10.1.1. Espionage targets in detail

Strategic information relevant to espionage against firms can be classified according to sectors of the economy or the departments of individual firms.

10.1.1.1. Sectors of the economy

It is perfectly obvious that information in the following sectors is of particular interest: biotechnology, genetic technology, medical technology, environmental technology, high-performance computers, software, optoelectronics, image sensing and signalling systems, data storage systems, industrial ceramics, high-performance alloys and nanotechnology. The list is not comprehensive and changes constantly in line with technological developments. In these sectors of industry, espionage primarily involves stealing research findings or details of special production techniques.

10.1.1.2. Departments of individual firms

The following departments are logical espionage targets: research and development, procurement, personnel, production, distribution, sales, marketing, product lines and finance. The significance and value of such information is often underestimated (see Chapter 10, 10.1.14).

[204] Information for firms provided with security protection, Federal Ministry of Economic Affairs, 1997.

10.1.2. Competitive intelligence

The strategic position of a firm on the market depends on its capabilities in the following spheres: research and development, production procedures, product lines, funding, marketing, sales, distribution, procurement and personnel[205]. Information on these capabilities is of major interest to any of the firm's competitors, since it gives an insight into the firm's plans and weaknesses and enables rivals to take strategic countermeasures.

Some of this information is publicly available. There are highly specialised consultancies, including such respected firms as Roland & Berger in Germany, which draw up, on an entirely legal basis, analyses of the competitive position on a given market. In the USA competitive intelligence has now become a standard management tool[206]. Professional analysis can turn a wide range of individual items of information into a clear picture of the situation as a whole.

The transition from legality to a criminal act of competitive intelligence is bound up with the choice of means used to obtain information. Only if the means employed are illegal under the laws of the country concerned do efforts to obtain information become a criminal act – the provision of analyses is not in itself punishable under the law. Naturally enough, information of particular interest to competitors is protected and can only be obtained by criminal means. The techniques employed for this purpose are in no way different from the general espionage methods described in Chapter 2.

No precise details are available concerning the scale of competitive intelligence operations. As in the case of conventional espionage, the official figures represent only the tip of the iceberg. Both parties concerned (perpetrator and victim) are keen to avoid publicity. Espionage is always damaging to the image of the firms concerned and the assailants naturally have no interest in public light being shed on their activities. For that reason, very few cases come to court.

Nevertheless, reports dealing with competitive intelligence repeatedly appear in the press. In addition, your rapporteur has discussed this issue with the heads of security of a number of large German firms[207] and with managers of US and European firms. The conclusion to be drawn is that cases of competitive intelligence repeatedly come to light, but do not determine firms' day-to-day behaviour.

10.2. Damage caused by industrial espionage

In view of the high number of unrecorded cases, it is difficult to determine precisely the extent of the damage caused by competitive intelligence/industrial espionage. In addition, some of the figures quoted are inflated because of vested interests. Security firms and counter-intelligence services have an understandable interest in putting the losses at the high end of the realistically possible scale. Despite this, the figures do give some idea of the problem.

[205] *Michael E. Porter*, Competitive Strategy, Simon & Schuster (1998).
[206] *Roman Hummelt*, Industrial espionage on the data highway, Hanser Verlag (1997).
[207] Details and names confidential.

As early as 1988, the Max Planck Institute estimated that the damage caused by industrial espionage in Germany amounted to at least DM 8 billion[208]. The chairman of the association of security consultants in Germany, Klaus-Dieter Matschke, quotes a figure of DM 15 bn a year, based on expert evidence. The President of the European police trade unions, Hermann Lutz, puts the damage at DM 20 bn a year. According to the FBI[209], US industry suffered losses of US$ 1.7 bn as a result of competitive intelligence and industrial espionage in the years 1992/1993. The former chairman of the Secret Service monitoring committee of the House of Representatives in the USA has spoken of losses of US$ 100 bn sustained through lost contracts and additional research and development costs. It is claimed that between 1990 and 1996 this resulted in the loss of 6 million jobs[210].

Basically the exact scale of the losses is irrelevant. The state has an obligation to combat competitive intelligence and industrial espionage using the police and counter-intelligence services, irrespective of the level of damage to the economy. Similarly, decisions taken by firms on the protection of information and counter-espionage measures cannot be based on total damage figures. Every firm has to calculate for itself the maximum possible damage as a result of the theft of information, assess the likelihood of such events occurring and compare the potential losses with the costs of security. The real problem is not the lack of accurate figures for the overall losses, the position is rather that such cost/benefit calculations are rarely carried out, except in large firms, and consequently security is disregarded.

10.3. Who carries out espionage?

According to a study by the auditors Ernest Young LLP[211], 39% of industrial espionage is carried out on behalf of competitors, 19% for clients, 9% for suppliers and 7% for secret services. Espionage is carried out by company employees, private espionage firms, paid hackers and secret service professionals[212].

10.3.1. Company employees (insider crime)

According to the literature examined, the expert evidence presented to the committee and the rapporteur's discussions with heads of security and counter-espionage authorities, there is a consensus that the greatest risk of espionage arises from disappointed and dissatisfied employees. As employees of the firm, they have direct access to information, can be recruited for money and will spy on their employer to obtain industrial secrets for those who hire them.

Major risks also arise when employees change jobs. Today it is not necessary to copy mountains of paper in order to take important information out of the firm. Such information can be stored on diskettes unnoticed and taken to the new employer when employees change job.

[208] Impulse, 3/97, 13 et seq.
[209] *Louis J. Freeh*, Director FBI, Statement for the Record, Hearing on Economic Espionage, House Judiciary Committee, Subcommittee on Crime, Washington DC, 9.5.1996
[210] *Robert Lyle*, Radio Liberty/Radio Free Europe, 10.2.1999.
[211] Computerzeitung, 30.11.1995, 2.
[212] *Roman Hummelt*, Spionage auf dem Datenhighway, Hanser Verlag (1997), 49 et seq.

10.3.2. Private espionage firms

The number of firms specialising in espionage is on the increase. Former members of the intelligence services sometimes work in these firms. Frequently the firms concerned also operate as security consultants and as detective agencies employed to obtain information. In general, the methods used are legal but there are also firms which employ illegal means.

10.3.3. Hackers

Hackers are computer specialists with the knowledge to gain access to computer networks from the outside. In the early days, hackers were computer freaks who got a kick out of breaking through the security devices of computer systems. Nowadays there are contract hackers in both the services and on the market.

10.3.4. Intelligence services

Since the end of the Cold War, the focus of the intelligence services' work has shifted. International organised crime and economic data are among their new tasks (for further details see Chapter 10, 10.5).

10.4. How is espionage carried out?

According to information provided by the counter-intelligence authorities and by the heads of security of large firms, all tried and tested intelligence service methods and instruments are used for the purposes of industrial espionage (see Chapter 2, 2.4). Firms have a more open structure than military and intelligence service facilities or government entities. In connection with industrial espionage, they are therefore exposed to additional risks:

- the recruitment of employees is simpler, as the facilities available to industrial security services cannot be compared to those of the counter-intelligence authorities;

- workplace mobility means that important information can be taken around on a laptop. The theft of laptops or the secret copying of hard disks after hotel room break-ins is thus one of the standard methods of industrial espionage;

- it is easier to break into firm's computer networks than those of security-sensitive State bodies, as small and medium-sized firms in particular have much less developed security awareness and security precautions;

- local tapping of communications (see Chapter 3, 3.2) is also easier for the same reasons.

Evaluation of the information gathered on this matter shows that industrial espionage is mainly carried out locally or through mobile workstations, as with a few exceptions (see Chapter 10, 10.6) the information sought cannot be obtained by intercepting international telecommunications networks.

10.5. Industrial espionage by states

10.5.1. Strategic industrial espionage by the intelligence services

After the end of the Cold War, intelligence service capacity was released and it can now be used more than before in other areas. The United States readily admits that some of its intelligence service's activities also concern industry. This includes, for example, monitoring of the observance of economic sanctions, compliance with rules on the supply of weapons and dual-use goods, developments on commodities markets and events on the international financial markets. The rapporteur's findings are that the US services are not alone in their involvement in these spheres, nor is there any serious criticism of this.

10.5.2. Intelligence services as agents of competitive intelligence

Criticism is levelled when state intelligence services are misused to put firms within their territory at an advantage in international competition through espionage. A distinction has to be made here between two cases[213].

10.5.2.1. High-tech states

Highly-developed industrial states can indeed gain advantage from industrial espionage. By spying on the stage of development reached in a specific sector, it is possible to take foreign trade and subsidy measures either to make domestic industry more competitive or to save subsidies. Another focus of such activities may be efforts to obtain details of particularly valuable contracts (see Chapter 10, 10.6).

10.5.2.2. Technologically less-advanced states

Some of these states are concerned to acquire technological know-how to enable their own industry to catch up without incurring development costs and licence fees. The aim may also be to acquire product designs and production methods in order to be able to compete on the world market with copies produced more cheaply by virtue of lower wages. There is evidence that the Russian intelligence services have been instructed to carry out such tasks. The Russian Federation's Law No 5 on foreign intelligence specifically mentions obtaining industrial and scientific/technical information as one of the intelligence service's tasks.

Another group of states (for example Iran, Iraq, Syria, Libya, North Korea, India and Pakistan) are concerned to acquire information for their national arms programmes, particularly in the nuclear sector and in the area of biological and chemical weapons. A further aspect of the activities of the services of these states is the operation of front companies which can purchase dual-use goods without raising suspicion.

[213] Confidential statement to the rapporteur by a counter-intelligence service, source protected.

10.6. Is ECHELON suitable for industrial espionage?

The strategic monitoring of international telecommunications, can produce useful information for industrial espionage purposes, but only by chance. In fact, sensitive industrial information is primarily to be found in the firms themselves, which means that **industrial espionage is carried out primarily by attempting to obtain the information via employees** or infiltrators or by breaking into internal computer networks. Only where sensitive data is sent outside via cable or radio (satellite) can a communications surveillance system be used for industrial espionage. This occurs systematically in the following three cases:

- in connection with firms which operate in three times zones, so that interim results are sent from Europe to America and then on to Asia;

- in the case of videoconferences in multinational companies conducted by VSAT or cable;

- when important contracts have to be negotiated locally (construction of facilities, telecommunications infrastructure, rebuilding of transport systems, etc.), and the firm's representatives have to consult their head office.

If firms fail to protect their communications in such cases, interception can provide competitors with valuable data.

10.7. Published cases

There are some cases of industrial espionage and/or competitive intelligence which have been described in the press or in the relevant literature. Some of these sources have been analysed and the results are summarised in the following table. Brief details are given of the persons involved, when the cases occurred, the detailed issues at stake, the objectives and the consequences.

It is noticeable that sometimes a single case is reported in very different ways. One example is the Enercom case, in connection with which either the NSA, or the US Department of Commerce or the competitor which took the photographs is described as the 'perpetrator'.

Case	Who	When	What	How	Aim	Consequences	Source
Air France	DGSE	Until 1994	Conversations between travelling businessmen	Bugs were discovered in the first class cabins of Air France aircraft – public apology by the company	Obtaining information	Not stated	„Wirtschaftsspionage: Was macht eigentlich die Konkurrenz?“ von Arno Schütze, 1/98
Airbus	NSA	1994	Information on an order for aircraft concluded between Airbus and the Saudi Arabian national airline	Interception of faxes and telephone calls between the negotiating parties	Forwarding of information to Airbus's US competitors, Boeing and McDonnell-Douglas	The Americans won the contract (US$ 6 bn)	„Antennen gedreht“, Wirtschaftswoche Nr.46 / 9 November 2000
Airbus	NSA	1994	Contract with Saudi Arabia worth US$ 6 bn uncovering of bribes paid by the European Airbus Consortium	Interception of faxes and telephone calls, routed via telecommunications satellites, between Airbus Consortium and the Saudi Arabian national airline/Government	Uncovering of bribes	McDonnel-Douglas, Airbus's American competitor, won the contract	Duncan Campbell in STOA 1999, Part 2/5, with reference to Baltimore Sun, America's Fortress of Spies, by Scott Shane and Tom Bowman, 3 December 1995, and Washington Post, Recent US Coups in New Espionnage, by William Drozdiak
BASF	Marketing manager	Not stated	Description of the process for the production of a raw material for skin creams by BASF (cosmetics division)	Not stated	Not stated	None, because the attempt was discovered	„Nicht gerade zimperlich“, Wirtschaftswoche Nr.43 / 16 October 1992
Federal German Ministry of Economic Affairs	CIA	1997	Information concerning high-tech products held by the Federal Ministry for Economic Affairs	Use of an agent	Obtaining information	Agent unmasked and expelled from the country	„Wirtschaftsspionage: Was macht eigentlich die Konkurrenz?“ von Arno Schütze, 1/98
Federal German Ministry of Economic Affairs	CIA	1997	Background to the Mykonos trial in Berlin, Hermes loans concerning exports to Iran, setting-up of German firms supplying high-tech products to Iran	CIA agent disguised as US Ambassador holds friendly conversations with the Head of the Department in the Federal Ministry for Economic Affairs responsible for the Arab region (particular responsibility: Iran)	Obtaining information	Not stated Civil servant contacts the German security authorities, who inform the Americans that the CIA operation is unwelcome. CIA agent then 'withdrawn'.	Industrial espionage. Firms as a target for foreign intelligence services, Baden-Württemberg Constitutional Protection Agency, Stuttgart as at 1998
Dasa	Russian Intelligence Service	1996 – 1999	Purchase and forwarding of armaments-related documents drawn up by a Munich arms firm (according to SZ of 30.05.2000: arms firm Dasa in Ottobrunn)	2 Germans working on behalf of the Russians	Obtaining information on guided missiles, armaments systems (anti-tank and anti-aircraft missiles)	SZ / 30.05.2000: '(...) Betrayal of secrets 'not particularly serious' from a military point of view. The court ruled that this also applied to the economic damage suffered.'	„Anmerkungen zur Sicherheitslage der deutschen Wirtschaft“, ASW; Bonn, April 2001 „Haftstrafe wegen Spionage für Russland“, SZ / 30 May 2000
Embargo	FIS	Around 1990	Resumption of exports of embargoed technology to Libya (e.g. by Siemens)	Interception of telephone calls	Uncovering illegal arms and technology transfer	No particular consequences, deliveries not prevented	'Maulwürfe in Nadelstreifen', Andreas Förster, p. 110

Case	Who	When	What	How	Aim	Consequences	Source
Enercon	Wind power expert from Oldenburg, Kenetech employee	Not stated	Wind-power plant developed by Enercon, a firm located in Aurich	Not stated	Not stated	Not stated	„Anmerkungen zur Sicherheitslage der deutschen Wirtschaft“, ASW; Bonn, April 2001
Enercon	NSA	Not stated	Wind wheel for electricity generation, developed by Aloys Wobben, an engineer from East Frisia	Not stated	Forwarding of technical details of Wobben's wind wheel to a US firm	US firm patents the wind wheel before Wobben; (breach of patent rights)	„Aktenkrieger“, SZ, 29 March 2001
Enercon	US firm Kenetech Windpower	1994	Important details of a high-tech wind-powered electricity generating plant (from switch gears to sails)	Photographs	Successful patent application in the USA	Enercon abandons its plans to attack the US market	„Sicherheit muss künftig zur Chefsache werden“, HB, 29 August 1996
Enercon	Engineer W., from Oldenburg, and US firm Kenetech	March 1994	Type E-40 wind-powered electricity generator developed by Enercon	Engineer W. passes on details, Kenetech employee photographs the plant and electrical components	Kenetech seeking evidence for legal action against Enercon for breach of patent rights on the grounds that Enercon had obtained commercial secrets illegally, According to an NSA employee, detailed information concerning Enercon was passed on to Kenetech via ECHELON	Not stated	„Klettern für die Konkurrenz“, SZ, 13 October 2000
Enercon	Kenetech Windpower	Before 1996	Data concerning Enercon's wind-powered electricity generating plant	Kenetech engineers photograph the plant	Kenetech copies the plant	Enercon vindicated; legal action brought against spy; estimated loss: several hundred million DM	„Wirtschaftsspionage: Was macht eigentlich die Konkurrenz?“ von Arno Schütze, 1/98
Japanese Trade Ministry	CIA	1996	Negotiations on import quotas for US cars on the Japanese market	Hacking into computer system of the Japanese Trade Ministry	US negotiator Mickey Kantor should accept lowers offer	Kantor accepts lowest offer	„Wirtschaftsspionage: Was macht eigentlich die Konkurrenz?“ von Arno Schütze, 1/98
Japanese cars	US Government	1995	Negotiations on the import of Japanese luxury cars Information on the emissions standards of Japanese cars	COMINT, no detailed information	Obtaining information	No details	Duncan Campbell in STOA, Part 2/5, 1999, with reference to Financial Post, Canada, 28 February 1998

Case	Who	When	What	How	Aim	Consequences	Source
López	NSA	Not stated	Videoconference involving VW and López	Interception from Bad Aibling	Forwarding of information to General Motors and Opel	The interception operation allegedly provided the State Prosecutor's Office with 'very detailed evidence' for its investigation	Bundeswehr Captain Erich Schmidt-Eenboom, quoted in 'Wenn Freunde spionieren' www.zdf.msnbc.de/news/54637.asp?cp1=1
López	López and three of his staff	1992 - 1993	Papers and information concerning research, planning, manufacturing and purchasing (documents concerning a plant in Spain, cost information for various model ranges, project studies, purchasing and saving strategies)	Collecting information	Use of General Motors documents by VW	Out of court settlement. In 1996, López resigns as VW manager, pays US$ 100 m to GM/Opel (supposedly lawyers' fees) and over a seven-year period purchases spare parts for a total of US$ 1 bn.	Industrial espionage. Firms as a target for foreign intelligence services, Baden-Württemberg Constitutional Protection Agency, Stuttgart as at 1998
López	NSA	1993	Videoconference between José Ignacio López and VW boss Ferdinand Piëch	Videoconference recorded and forwarded to General Motors (GM)	Protection of commercial secrets held by GM in America, secrets which López wished to pass on to VW (price lists, secret plans for a new car plant and a new small car)	López's cover is blown, in 1998 criminal proceedings are halted in return for payment of fines. No consequences in respect of NSA	„Antennen gedreht“, Wirtschaftswoche Nr.46 / 9 November 2000 „Abgehört“, Berliner Zeitung, 22 January 1996 „Die Affäre López ist beendet“, Wirtschaftsspiegel, 28 July 1998 „Wirtschaftsspionage: Was macht eigentlich die Konkurrenz?“ von Arno Schütze, 1/98
Los Alamos	Israel	1988	Two employees of the Israeli nuclear research programme hack into the central computer of the Los Alamos nuclear weapons laboratory	Hacking	Obtaining information about new fuses for US atomic weapons	No specific consequences, since the hackers fled to Israel. One is briefly held in custody in Israel, links with the Israeli Secret Service are not officially confirmed	'Maulwürfe in Nadelstreifen', Andreas Förster, p. 137
Smuggling	FIS	1970s	Smuggling of computers into the GDR	Not stated	Uncovering of technology transfer to the Eastern Bloc	No particular consequences, deliveries not prevented	'Maulwürfe in Nadelstreifen', Andreas Förster, p. 113

Case	Who	When	What	How	Aim	Consequences	Source
TGV	DGSE	1993	Cost calculation by Siemens Contract to supply high-speed trains to South Korea	Not stated	Lower price offer	The manufacturer of the ICE loses the contract to Alcatel-Alsthom	„Wirtschaftsspionage: Was macht eigentlich die Konkurrenz?“ von Arno Schütze, 1/98
TGV	Unknown	1993	Cost calculation by AEG and Siemens concerning a government contract to supply South Korea with high-speed trains	Siemens claims that the telephone and fax connections in its Seoul office are being tapped	Negotiating advantage for the Anglo-French competitor GEC Alsthom	South Korea decides in favour of GEC Alsthom, although the German offer was initially regarded as better	„Abgehört“, Berliner Zeitung, 22 January 1996
Thomson-Alcatel v Raytheon	CIA/ NSA	1994	Award to the French firm Thomson-Alcatel of a Brazilian contract for the satellite monitoring of the Amazon Basin (US$ 1.4 bn)	Interception of communications to and from the successful tenderer (Thomson-Alcatel)	Uncovering corruption (payment of bribes)	Clinton complains to the Brazilian Government; under pressure from the US Government, the contract is awarded to the US firm Raytheon	'Maulwürfe in Nadelstreifen', Andreas Förster, p. 91
Thomson-Alcatel v Raytheon	US Department of Commerce 'made efforts'	1994	Negotiations on a project worth billions of dollars concerning the radar monitoring of the Brazilian rainforest	Not stated	Win contract	The French firms Thomson CSF and Alcatel lose the contract to the US firm Raytheon	„Antennen gedreht“, Wirtschaftswoche Nr.46 / 9 November 2000
Thomson-Alcatel v Raytheon	NSA Department of Commerce		Negotiations concerning a project worth US$ 1.4 bn concerning the monitoring of Amazon Basin (SIVA) Discovery that the Brazilian selection panel had accepted bribes. Comment by Campbell: Raytheon supplies equipment for the Sugar Grove interception station	Surveillance of the negotiations between Thomson-CSF and Brazil and forwarding of the findings to Raytheon Corp.	Uncovering bribery Winning of the contract	Raytheon wins the contract	Duncan Campbell in STOA, 1999, Part 2/5, with reference to New York Times, How Washington Inc. Makes a Sale, by David Sanger, 19 February 1995, and http://www:raytheon:com/sivam/contract:html
Thyssen	BP	1990	Gas and oil drilling contract in the North Sea worth millions of dollars	Interception of faxes sent by the successful tenderer (Thyssen)	Uncovering corruption	BP brings an action for damages against Thyssen	'Maulwürfe in Nadelstreifen', Andreas Förster, p. 92
VW	Unknown	'recent years'	Not stated	Inter alia, infrared camera, fixed in a mound of earth, which transmits images by radio	Obtaining information about new developments	VW admits losses of profits totalling hundreds of millions of deutschmarks	„Sicherheit muss künftig zur Chefsache werden“, HB / 29 August 1996
VW	Unknown	1996	VW test circuit in Ehra-Lessien	Hidden camera	Information about new VW models	Not stated	„Auf Schritt und Tritt“ Wirtschaftswoche Nr. 25, 11 June 1998

10.8. Protection against industrial espionage

10.8.1. Legal protection

The legal systems of all the industrialised countries define the theft of commercial secrets as a criminal offence. As in all other areas of the criminal law, the degree of protection varies from country to country. As a rule, however, the penalties for industrial espionage are much less severe than those for espionage in connection with military security. In many cases, competitive intelligence operations are banned only against firms from the same country, but not against foreign firms abroad. This is also the case in the USA.

In essence, the relevant laws prohibit only espionage by one industrial undertaking against another. It is doubtful whether they also restrict the activities of state intelligence services, since, on the basis of the laws establishing them, the latter are authorised to steal information.

A grey area develops if intelligence services seek to pass on to individual firms information gained by means of espionage. The laws which endow intelligence services with special powers would normally not cover such activities. In particular, in the EU this would represent a breach of the EEC Treaty.

Irrespective of this fact, however, in practice it would be very difficult for a firm to seek legal protection by bringing an action before the courts. Interception operations leave no trace and generate no evidence which might be used in court.

10.8.2. Other obstacles to industrial espionage

States accept the fact that intelligence services, in keeping with their general objective of securing strategic information, are also active in the commercial sphere. However, this gentlemen's agreement is frequently breached in connection with competitive intelligence operations designed to benefit a country's own industry. Any state caught red-handed comes under massive political pressure. This applies in particular to a world power such as the USA, whose claim to global political leadership would be drastically undermined. Middle-ranking powers could probably afford to be singled out for such activities; a superpower certainly cannot.

Alongside the political problems, there is also the practical issue of which individual firm is to be provided with the information gained by means of competitive intelligence operations. In the aerospace sector, the answer is a simple one, because the global market is dominated by only two major firms. In all other cases where a market is supplied by a number of firms which are not state-controlled, it is extremely difficult to give preference only to one. In connection with international contract-award procedures, an intelligence service is more likely to forward detailed information concerning other competitors' offers to all the participating firms from its own country, rather than simply to one. This applies in particular when all the participating firms from one country can draw on the same level of government support, as is the case in the USA through the work of the Advocacy Center. In the case of the theft of technology, which should necessarily lead to the registration of a patent, it is only logical that such equal treatment would no longer be possible.

Moreover, under the US political system in particular this would give rise to a serious problem. US politicians are massively dependent on contributions from firms in their constituencies to finance their election campaigns. If proof were to emerge of even one case of intelligence services favouring individual firms, the upheaval in the political system would be massive. As the former CIA Director James Woolsey put it in a discussion with representatives of the committee: 'In that case the Hill (i.e. the US Congress) would go mad!'. Quite!

10.9. The USA and economic matters in the post-Cold War era

Since 1990, the US Administration has increasingly come to equate national security with economic security. The annual White House report entitled 'National Security Strategy' repeatedly emphasises that **'economic security is fundamental not only to our national interests, but also to national security'**.

This development can be traced back to a number of sources. Essentially, three factors came together:

- the interest of the intelligence services in taking on a task which would outlive the Cold War;
- the US State Department's simple acknowledgement of the fact that, following the Cold War, the USA's leading role in the world could not be based solely on military strength, but also made economic strength essential;
- President Clinton's interest, from a domestic policy point of view, in strengthening the US economy and creating jobs.

This combination of interests had practical consequences.

As a logical response, since 1992, the FBI has focused its counterintelligence activities on industrial espionage and, in 1994, it set up an Economic Counterintelligence Program. Speaking to the US Congress, Louis J. Freeh, the Director of the FBI, described this as a **defensive** programme designed to prevent the competitiveness of the US economy from being undermined by the theft of information.

As a logical response, at least from an American point of view, the Administration has used the CIA, and subsequently the NSA, to prevent distortions of competition by means of bribery. The former Director of the CIA, James Woolsey, made this explicitly clear at a press conference he gave on 7 March 2000 at the request of the US State Department[214].

As a logical response, the US Department of Commerce has focused its efforts to foster exports in such a way that a US firm wishing to export goods need only deal with one agency. Active use is made of all the weapons at the Administration's disposal (for further details, see Chapter 10, 10.9.4).

[214] State Department Foreign Press Center briefing, Subject: Intelligence Gathering and Democracies: The Issue of Economic and Industrial Espionage, Washington DC, 7.3.2000

10.9.1. The challenge for the US Administration: industrial espionage against US firms

Intelligence operations directed against the US economy are neither unusual nor new. For decades, both the USA and other leading industrialised countries have been targets for industrial espionage. During the Cold War, however, economic and technological intelligence-gathering took second place to conventional espionage. Following the end of the Cold War, industrial espionage has come into its own[215].

In 1996, speaking to the US Congress, the Director of the FBI, Louis J. Freeh, gave a detailed account of the way the US economy has become a target for industrial espionage by other countries' intelligence agencies. As he put it, 'consequently foreign governments, through a variety of means, actively target US persons, firms, industries and the US Administration itself, to steal or wrongfully obtain critical technologies, data and information in order to provide their own industrial sectors with a competitive advantage'. However, the theft of information by Americans was increasing just as much. The further remarks made by Mr Freeh to the US Congress are summarised below. At this point, your rapporteur would like to express regret at the fact that the US Administration did not allow a delegation from the Temporary Committee to discuss these issues with the FBI. Up-to-date information could then have been obtained. In the paragraphs which follow, therefore, your rapporteur has assumed that the US Administration takes the view that the hearing before the House of Representatives held in 1996 gives an accurate picture of the threat currently posed to the US economy by industrial espionage. Accordingly, he has drawn extensively on that source.

10.9.1.1. The players

At the time of the hearing, the FBI was investigating persons or organisations from 23 countries who were suspected of industrial espionage against the USA. Some ideological or military opponents of the USA have merely continued their Cold War activities[216]. In contrast, other governments carry out industrial and technological espionage, even though they have long been the USA's military and political allies. In so doing, they often exploit their ease of access to US information. Some have developed agencies which assess information concerning high-technology products and use that information in competition with US firms. No countries have actually been named, although the involvement of Russia, Israel and France has been hinted at[217].

10.9.1.2. Objectives of industrial espionage

The objectives of industrial espionage named by the FBI in no way differ from those outlined in Chapter 10, 10.1.1. However, high-technology products and the defence industry are given as priority objectives. Interestingly enough, the FBI names information concerning bids, contracts, clients and strategic information in these areas as objectives of industrial espionage

[215] Statement for the Record of *Louis J. Freeh*, FBI Director, Hearing on Economic Espionage, House Judiciary Committee, Subcommittee on Crime, Washington DC, 9.5.1996
[216] 'The end of the Cold War has not resulted in a peace dividend regarding economic espionage', Statement for the Record of *Louis J. Freeh*, FBI Director, Hearing on Economic Espionage, House Judiciary Committee, Subcommittee on Crime, Washington DC, 9.5.1996
[217] Interpretation by your rapporteur of the cryptic remarks made by *Louis J. Freeh* to the committee.

which are pursued **aggressively**[218].

10.9.1.3. Methods

In the context of the **Economic Counterintelligence Program**, the FBI has identified a series of espionage methods. A combination of methods is employed in most cases, a single method only rarely. According to the information obtained by the FBI, the best source is a person employed by a firm or organisation, something which is not only true for the USA (see Chapter 10, 10.3. and 10.4.). At the hearing, the FBI outlined how persons are used to carry out for espionage, but astonishingly gave no details of electronic methods.

10.9.2. The attitude of the US Administration towards active industrial espionage

At a press conference[219], and in a conversation with members of the committee in Washington, the former Director of the CIA, James Woolsey, briefly summarised the interception activities of the US Secret Service as follows:

1. The USA monitors international telecommunications in order to obtain general information about economic developments, shipments of dual-use goods and compliance with embargoes.

2. The USA monitors on a targeted basis communications by individual firms in connection with contract-award procedures in order to prevent corruption-related distortions of competition to the detriment of US firms. Questioned more closely, however, Woolsey gave no specific examples.

US firms are banned by law from payment bribes and accountants are required to report evidence of such payments. If a telecommunications surveillance operation reveals evidence of bribery in connection with public contracts, the US ambassador makes representations to the government of the country concerned. However, US firms competing for the contract are not directly informed. He categorically ruled out the possibility of espionage solely for the purposes of obtaining competitive intelligence.

At a hearing before the House Permanent Select Committee on Intelligence held on 12 April 2000, the current Director of the CIA, George J. Tenet, echoed Woolsey's comments: 'It is not the policy nor the practice of the United States to engage in espionage that would provide an unfair advantage to US companies'. At the same hearing, Tenet went on to say that information on the payment of bribes was forwarded to other government agencies so that they could help US firms[220]. In response to a supplementary question from Congressman Gibbons, Tenet admitted that there was no legal ban on the gathering of competitive

[218] In these areas the interception of communications is a promising method!

[219] *James Woolsey,* Remarks at the Foreign Press Center, Transcript, 7.3.2000, http://cryptome,org/echelon-cia.htm

[220] 'As I indicated also in my testimony, there are instances where we learn, that foreign companies or their governments bribe, lie, cheat or steal their way to disenfranchise American companies. When we generate this information, we take it to other appropriate agencies, make them aware of it. They use that information through other means and channels to see if they can assist an American company. But we play defence, we never play offense, and we never will play offense'.

intelligence; however, he saw no need for such a ban, given that the intelligence services were not involved in activities of that kind.

In the course of a conversation held with him in Washington, the chairman of the House Permanent Select Committee on Intelligence, Porter Goss, painted a similar picture of US interception activities.

10.9.3. Legal situation with regard to the payment of bribes to public officials[221]

The payment of bribes to secure contracts is a worldwide, and not simply European, phenomenon. According to the Bribe Payers Index (BPI) published by Transparency International in 1999, which ranks the 19 leading exporting countries on the basis of their willingness to offer bribes, Germany and the USA share ninth place. Sweden, Austria, The Netherlands, the United Kingdom and Belgium were identified as being less likely to offer bribes; only Spain, France and Italy have a higher rating[222].

The Americans refer to the corrupt practices employed by European firms to justify industrial espionage. This is questionable, not only because wrongdoings by individual firms cannot justify the comprehensive use of espionage. Such heavy-handed practices could only be tolerated if there were a legal vacuum in this area.

However, the legal measures taken to combat corruption are just as stringent in Europe as they are in the USA. In 1997, these shared interests led to the adoption of the OECD Convention on Combating Bribery of Foreign Public Officials in International Business Transactions. The Convention requires the signatory states to make the payment of bribes to a foreign public official a criminal offence and contains, alongside a definition of the offence of bribery, provisions concerning penalties, jurisdiction and enforcement.

The Convention, which came into force on 15 February 1999, has been transposed and ratified by all the EU Member States except Ireland. The USA transposed the Convention by adopting the 1998 International Anti-Bribery and Fair Competition Act amending the Foreign Corrupt Practices Act (FCPA) of 1977, which imposes on firms a requirement to keep accounts and prohibits the payment of bribes to foreign public officials[223]. Neither in the USA nor in the EU Member States are bribes accepted as tax-deductible operating expenditure[224].

Whereas the OECD Convention is designed only to combat the payment of bribes to foreign public officials, in 1999 the Council of Europe adopted two more far-reaching agreements,

---

[221] *Albin Eser, Michael Überhofer, Barbara Huber* (Eds), Using the criminal law to combat corruption. A comparative survey of offences involving bribery, drawn up on behalf of the Bavarian Ministry of Justice, edition iuscrim (1997).

[222] The scale runs from 10 (low incidence of bribery) to 0 (high incidence of bribery): Sweden (8.3), Australia (8.1), Canada (8.1), Austria (7.8), Switzerland (7.7), Netherlands (7.4), United Kingdom (7.2), Belgium (6.8), Germany (6.2), USA (6.2), Singapore (5.7), Spain (5.3), France (5.2), Japan (5.1), Malaysia (3.9), Italy (3.7), Taiwan (3.5), South Korea (3.4) and China (3.1).
http://www.transparency.org/documents/cpi/index.html#bpi

[223] OFFICE OF THE CHIEF COUNSEL FOR INTERNATIONAL COMMERCE, Legal Aspects of International Trade and Investment, http://www.ita.doc.gov/legal/

[224] http://www.oecd.org/daf/nocorruption/annex3.htm

although neither has yet come into force. The Criminal Law Convention on Corruption[225] also encompasses bribery in the private sector. It was signed by all the EU Member States except Spain and by the USA, but as yet has been ratified only by Denmark.

The Civil Law Convention on Corruption[226] lays down rules governing liability and compensation, stipulating in particular that contracts and contract clauses which require firms to pay bribes will be deemed null and void. It has been signed by all the EU Member States except the Netherlands, Portugal and Spain; the USA has not signed.

The EU has adopted two further legal acts designed to combat bribery: the Convention on the fight against corruption involving officials and the Joint Action on corruption in the private sector.

The Convention on the fight against corruption involving officials of the European Communities or officials of the EU Member States[227] is designed to ensure that corruption and the payment of bribes to officials are criminal offences throughout the EU. The Member States undertake to make both the payment of bribes to an official and corruption criminal offences, regardless of whether one of their own officials, an official of another Member State or an EU official is involved.

The Joint Action on corruption in the private sector[228] is intended to ensure that corruption and the payment of bribes to firms are criminal offences. In that connection, criminal law penalties are laid down for both natural and legal persons. However, the scope of the Joint Action is more restricted than that of the Convention on the fight against bribery involving officials in that it requires the Member States only to punish actions carried out at least in part on their territory. Member States are free to extend this jurisdiction to cover actions carried out abroad by their own nationals or to the benefit of domestic legal persons. Germany and Austria have made instances of corruption carried out abroad criminal offences provided that they are also punishable in the country concerned.

10.9.4. The role of the Advocacy Center in promoting US exports

By means of Executive Order 12870, in 1993 President Clinton set up the Trade Promotion Coordinating Committee (TPCC)[229]. Its role is to coordinate and develop a strategy for the US Administration's trade promotion policy. In accordance with the Executive Order, a representative of the National Security Council (NSC) also sits on the TPCC[230]. The NSC formulates the United States' national security policy with reference to domestic policy, foreign policy, military and intelligence issues. Each president alters the focus of the NSC's

[225] Criminal Law Convention on Corruption http://conventions.coe.int/treaty/EN/WhatYouWant.asp?NT=173&CM=8&DF=21/06/01

[226] Civil Law Convention on Corruption ETS no.: 174, http://conventions.coe.int/treaty/EN/WhatYouWant.asp?NT=174&CM=8&DF=21/06/01

[227] Convention, drawn up on the basis of Article K.3(2)(c) of the Treaty on European Union, on the fight against corruption involving officials of the European Communities or officials of Member States of the European Union, OJ C 195, 25.6.1997, 2.

[228] Joint Action of 22 December 1998 adopted by the Council on the basis of Article K.3 of the Treaty on European Union, on corruption in the private sector (98/742/JHA), OJ L 358, 31.12.1998, 2.

[229] White House Archive, http://govinfo.library.unt.edu/npr/library/direct/orders/tradepromotion.html

[230] Homepage of the National Security Council (NSC), http://www.whitehouse.gov/nsc

work. On 21 January 1993, by means of PDD2, President Clinton expanded the NSC and, at the same time, placed more emphasis on economic issues in connection with the formulation of security policy. Members of the NSC include the President, the Vice-President, the Secretary of State and the Secretary of Defense. The Director of the CIA is an advisory member.

10.9.4.1. The task of the Advocacy Center

The Advocacy Center, which is attached to the US Department of Commerce, is at the heart of the national export strategy employed by President Clinton and continued by President Bush. It acts as the interface between the TPCC and the US economy. By its own account, since its inception in 1993 the Center has helped hundreds of US firms to win public contracts abroad.

The Advocacy Center helps US businesses by[231]:

- marshalling the resources of the US Administration - from the various financing, regulatory, country and sector experts, through the worldwide network of commercial officers, to the White House;
- fighting to level the playing field and promote open competition in the international bidding arena – from the multibillion dollar infrastructure project to the strategic contract for a small business;
- pursuing deals on behalf of US companies from start to finish, through 'hands-on' support;
- supporting US jobs and boosting US exports through the successes of US companies who successfully bid for overseas projects and contracts;
- assisting US firms with stalled negotiations due to foreign government inaction or 'red tape'.

10.9.4.2. The Advocacy's Center's operating methods[232]

Only the Director and a small staff complement of 12 persons work at the Center itself (situation as at 6 February 2001). The project managers cover the following areas: Russia and the newly independent countries; Africa, East Asia and the Pacific; the Middle East and North Africa; South Asia – Bangledesh, India, Pakistan, Sri Lanka; Europe and Turkey; China, Hong Kong and Taiwan; Canada, the Caribbean and Latin America; the aerospace, automobile and defence industries worldwide; and the telecommunications, IT and computer industries worldwide.

The Center provides firms with a central contact point for their dealings with the various US authorities involved in promoting exports. It works on behalf of firms on a non-discriminatory basis, but, in line with the clear rules governing its work, supports only projects which are in the US national interest. For example, projects manufactured in the USA must make up at least 50% of the value of the goods delivered under any given contract.

10.9.4.3. Involvement of the CIA in the work of the TPCC

[231] TPCC brochure on the Advocacy Center, October 1996

[232] Homepage of the Advocacy Center, http://www.ita.doc.gov/td/advocacy/

Duncan Campbell submitted to the members of the Temporary Committee a number of declassified documents which provide evidence of CIA involvement in the work of the Advocacy Center. They include minutes of the Trade Promotion Coordinating Committee dealing with a meeting of the Indonesia Working Group held in July and August 1994[233]. According to the documents, a number of CIA staff members sit on the Working Group, whose task is to draw up a trade strategy for Indonesia. The CIA staff members are named in the minutes.
Moreover, the minutes show that one of the CIA staff members defines one objective of the Working Group as that of identifying main competitors and making this background information available to firms[234].

10.9.4.4. Open questions in connection with the Advocacy Center

The US Administration did not allow the discussion arranged between members of the Temporary Committee and representatives of the Center to take place. For that reason, much to your rapporteur's regret, two areas of doubt could not be cleared up:

a. the Temporary Committee has in its possession documents which provide evidence of CIA involvement in the work of the TPCC (see Chapter 10, 10.9.4.3.),

b. in its own information brochure (quoted above), the Advocacy Center acknowledges that it focuses the resources of 19 'US government agencies'. Elsewhere in the brochure, however, only 18 such agencies are listed, raising the issue of why the 19th cannot be named in public.

Your rapporteur can only assume that the discussion arranged with the Advocacy Center was cancelled because it is involved in activities which the US Administration wishes to keep secret.

10.10. Security of computer networks

10.10.1. The importance of this chapter

As already outlined in Chapter 10, 10.4., nowadays, alongside the use of spies, hacking into computer networks or the theft of data from laptop computers represents the second most effective method of industrial espionage. The information given in this chapter has no direct bearing on the existence or otherwise of a global system for the interception of international communications. However, in view of the Temporary Committee's aims, the chapter on industrial espionage must include brief details of one of its most powerful tools. This will certainly help readers to assess the significance of a system for the interception of international communications in connection with industrial espionage.

[233] TPCC Working Group Meeting, Agenda, 18.7.1994, TPCC Indonesia Advocacy-Finance Working Group, Distribution List, and Minutes of the meeting of 17.8.1994, from a letter from the US and Foreign Commercial Service of 25.8.1994.
[234] ibidem: 'Bob Beamer suggested that any primary competitors known to the group for these projects should be included as background information', Bob Beamer is one of the CIA representatives.

10.10.2. The risks inherent in the use by firms of modern information technology

Modern electronic data-processing technologies have been in common use by firms for some time now. Data of all kinds is stored in highly compressed form on a variety of media. Data stored on computer has now become one of the key aspects of commercial know-how. This transition from an industrial to an information society is opening up new opportunities, but, at the same time, creating substantial security risks[235].

10.10.2.1. The risks are increasing

The new risks which are emerging can be summarised as follows[236]:
More and more firms have computer networks and more and more information is being condensed in one place, with the result that it can be copied simply by hacking into the network. At the same time, other sensitive items of information are being decentralised and are thus not easily accessible in the context of a centralised security management strategy. The mobility of senior managers, who carry sensitive information with them on their laptop computers, is creating additional risks. The outsourcing of services is giving rise to new maintenance practices in the IT sphere as well which are highly questionable from a security point of view. A combination of the low status accorded to security staff in firms' management hierarchy and senior managers' ignorance of security issues is giving rise to misguided decisions.

10.10.2.2. Some of the risks in detail

Compression of information on compact media
Nowadays, firms' business secrets are stored in a physically very small area on compressed media. As a result, for example, the full plans for a new factory can be smuggled out of a firm on a substitute hard disk the size of a cigarette packet or copied electronically in minutes, without leaving any trace, by hacking into a computer network.

Decentralisation of secret information
In the era of large-scale computers, it was easy to monitor access to secret information, since only one computer was involved. Today, each employee connected to the network is provided with substantial computing capacity at his or her workstation. This is of course a great advantage for the staff member concerned, but a disaster from a security point of view.

Easier copying of information
In the era of hand-drawn plans and mechanical typewriters it was very difficult to copy large numbers of documents without being detected. Today, in the electronic era, it is easy. Large volumes of digitalised information can be copied easily, quickly and without leaving any trace. As a result, in many cases only one intervention is needed to obtain the material in question and the risk of being detected is correspondingly much lower.

Mobility of senior managers
Often without being properly aware of the fact, senior managers often carry strategically

[235] Computer espionage, Document 44, Federal Ministry for Economic Affairs, July 1998.
[236] *Roman Hummelt*, Industrial Espionage on the Data Highway, Hanser Verlag (1997).

important information about their firms with them on their laptop computers. The speed with which a copy of the hard disk can be made in the course of a 'customs check' or a search of a hotel room offers intelligence services substantial opportunities for action. Alternatively, the Notebook in question is simply stolen. Moreover, in view of the decentralisation involved it is difficult to incorporate into a central security management strategy the information stored on the hard disks of laptop computers used by a firm's senior managers.

Outsourcing of maintenance services
Although outsourcing may serve to reduce a firm's costs, in the sphere of information technology and the maintenance of telephone networks it allows technicians from outside the firm virtually unrestricted access to information. The associated risks cannot be over-emphasised.

Inadequate network administration
Alongside security loopholes in the software itself, which hackers repeatedly find, the most serious danger stems from network administrators who are not properly aware of the risks. In its basic form, Windows NT is configurated in such a way that it reveals almost all the information required for a successful attack on the network[237]. If these configurations and standard passwords are not changed, accessing the network is child's play. Firms often make the mistake of investing considerable amounts of time and money in the security of the firewall, but fail to protect the network properly against attacks from within[238].

10.10.3. Frequency of attacks on networks

The number of instances of computer networks being hacked into via the Internet is increasing every year[239]. In 1989, the Computer Emergency Response Team (CERT), an organisation set up in the USA in 1988 with the aim of improving Internet security, received notification of 132 security problems. In 1994, the figure had already risen to 2 241 and in 1996 it reached 2 573. The real figure is certainly much higher. This assumption was backed up by a large-scale simulation which the US Department of Defense carried out using its own computers. Systematic efforts were made to hack into 8 932 servers and mainframe computers from outside. In 7 860 cases these attempts proved successful, only 390 attempts were detected and no more than 19 cases were reported. A distinction must be drawn between attacks and security problems. An attack is a single attempt to gain unauthorised access to a system. A security problem consists of a number of related attacks. Extrapolating from their own long-term studies, the Pentagon and US universities have posited a figure of 20 000 security problems and 2 million attacks on the Internet annually.

10.10.4. Perpetrators and methods

The aim of foreign intelligence services which attack IT systems is to secure the information they contain, if at all possible without being detected. In principle, a distinction can be drawn between three groups of perpetrators with three different modi operandi.

In-house attackers with comprehensive access authorisation

[237] *George Kurtz, Stuart McClure, Joel Scambray,* Hacking exposed, Osborne/McGraw-Hill (2000), 94.
[238] *Martin Kuppinger,* Internet and Internet Security, Microsoft Press Deutschland (1998), 60.
[239] *Othmar Kyas,* Security on the Internet, International Thomson Publishing (1998), 23.

A spy who has been smuggled into a firm or whose services have been bought and who has risen to become a systems administrator or security administrator in a computer centre need only make extensive use of the powers officially granted to him in order to steal virtually all his employer's know-how. The same applies to a senior development engineer with unrestricted access authorisation to all a firm's databanks.

A spy of this kind offers maximum espionage effectiveness. However, if suspicions arise, the risk of detection is high, since the investigations immediately focus on the small group of persons who have comprehensive access to information. Moreover, it is pure coincidence if a spy secures comprehensive access authorisation.

In-house attackers with workstation access authorisation
A spy working within a firm has a clear advantage over a hacker attacking from the outside: he must overcome only the network security precautions, but no firewall. From an individual workstation, and provided that the person concerned has the requisite knowledge, the architecture of the network can be established and substantial volumes of information can be obtained, using the same techniques employed by an outside hacker and other techniques available only to persons working from within[240]. In addition, the spy can converse with colleagues without raising suspicion and obtain passwords by means of 'social engineering'.

The effectiveness of such a spy can be high, but is not as predictable as in the first case. The risk of detection is lower, particularly in the case of networks whose administrator pays little attention to the dangers of an attack from within. It is much easier to smuggle in a spy trained to hack into computer networks (trainees, guest researchers, etc.).

10.10.5. Attacks from outside by hackers

That hackers repeatedly gain unauthorised access to computer networks is well-known and well-documented. Intelligence services themselves now train specialists in the skills needed to hack into computer networks. The effectiveness of such an attack cannot be predicted or planned; it depends to a great extent on the effectiveness of the network defence mechanisms and on whether, for example, the network used by the research department is physically linked to the Internet. The level of risk involved for a professional spy is virtually zero; even if the attack is detected, the spy is somewhere else entirely.

10.11. Under-estimation of the risks

10.11.1. Risk-awareness in firms

As things stand, awareness of the risk of industrial espionage is not very well developed in individual firms. This is partly reflected in the fact that security officers often have middle-management rank and are not board members. However, security costs money and board members generally take an interest in security issues only when it is too late.

Large firms do at least have their own security departments and employ security specialists in the IT sphere as well. In contrast, small and medium-sized firms vary rarely employ security

[240] *Anonymous,* Hacker's guide, Markt & Technik-Verlag (1999).

experts and are generally happy enough if their data-processing equipment works properly. However, such firms as well may be targets for industrial espionage, since many of them are highly innovative. Moreover, in view of their integration in the production process medium-sized component suppliers offer a suitable basis for industrial espionage operations against large firms.

10.11.2. Risk-awareness among scientists

As a rule, researchers are interested only in their area of expertise and can therefore sometimes be an easy target for intelligence services. Your rapporteur has noted with some amazement that research institutes whose work has obvious practical applications communicate with each other using unencrypted e-mails and the science network. This is quite simply reckless.

10.11.3. Risk-awareness in the European institutions

10.11.3.1. European Central Bank

Information concerning preparations for decisions by the European Central Bank (ECB) could be of great value to intelligence services – and, it goes without saying, of course to the markets. At a meeting held in camera, the committee heard statements by representatives of the ECB concerning the security precautions taken to protect information. On that basis, your rapporteur has come to the conclusion that the ECB is aware of the risks and, as far as is feasible, is taking appropriate security measures. However, he has been supplied with information[241] suggesting that risk-awareness is low in certain national central banks.

10.11.3.2. Council of the European Union

Prior to the appointment of the High Representative for the common foreign and security policy, the Council focused its efforts in the area of secrecy on measures to keep information concerning decision-making procedures and the stances adopted by the Member State governments from the public and the European Parliament. It would have had no defence against a professional intelligence operation[242]. For example, technical maintenance in the interpreting booths was apparently carried out by an Israeli firm. The Council has now adopted security regulations[243] consistent with the standard within NATO.

10.11.3.3. European Parliament

Up to now, the European Parliament has never dealt with classified documents and therefore has no experience in the area of the protection of secrecy and no security culture. The need for such a culture will only arise if Parliament gains access to classified documents in the future. Otherwise, a general policy of secrecy is anathema for a parliament whose actions must be as transparent as possible. However, with a view to protecting informants and petitioners, provision should be made for the encryption of e-mails transmitted from one Member's office to another. At present, this is not possible.

10.11.3.4. European Commission

The European Commission has directorates-general which, by virtue of the information they deal with, have no need for secrecy rules or protection arrangements. Indeed, the reverse is

[241] Private information, source protected.
[242] Information supplied by members of COREPER and Council officials; sources protected.
[243] Council Decision of 19 March 2001 adopting the Council's security regulations, OJ L 101, 11.4.2001, 1.

true: complete transparency should be the norm in all areas which have a bearing on legislation. The European Parliament must employ a vigilant approach in order to ensure that, in these areas, the influence exerted on legislative proposals by interested firms, etc. is not masked even more than it already is through the unnecessary introduction of inappropriate secrecy rules.

Admittedly, there are areas of the Commission's work which involve the processing of sensitive information. Alongside Euratom, the most obvious areas are foreign relations, foreign trade and competition. On the basis of the information supplied by the directorates-general concerned to the committee at a meeting held in camera, and above all on the basis of other information available to your rapporteur, it is very doubtful as to whether the European Commission is properly aware of the risk of espionage and whether it takes a professional approach to the issue of security. Naturally enough, a public report is no place in which to outline security shortcomings. Nevertheless, your rapporteur sees a pressing need for the European Parliament to consider this issue in an appropriate manner.

However, it can be stated now that the encryption systems which the Commission employs when communicating with some of its external offices are outdated. This does not mean that the security standard is poor. However, the equipment currently in use is no longer manufactured and only roughly half of the external offices are equipped with encryption technology. The introduction of a new system working on the basis of encrypted e-mails is an urgent necessity.

11. Cryptography as a means of self-protection

11.1. Purpose and method of encryption

11.1.1. Purpose of encryption

Every time a message is transmitted, there is a risk of its falling into unauthorised hands. To prevent outsiders ascertaining its content in such cases, the message must be made impossible for them to read or intercept, i.e. encrypted. Consequently encryption techniques have been used since time immemorial for military and diplomatic purposes[244].

In the past 20 years the importance of encryption has increased, since an ever greater proportion of communications has been sent abroad, where the confidentiality of post and telecommunications could not be guaranteed by the state of origin. Moreover, the expanded technical opportunities for the state legally to intercept/record communications on its own territory has led to concern among ordinary citizens and a greater need for their protection. Finally, the increased interest among criminals in having illegal access to information, and the ability to falsify it, has also given rise to protection measures (e.g. in the banking sector).

The invention of electrical and electronic communications (telegraph, telephone, radio, telex, fax and Internet) greatly simplified the transmission of intelligence communications and made them immeasurably quicker. The downside was that there was no **technical** protection against interception or recording, so that anyone with the right equipment could read the communication if he could gain access to the means of communication. If done professionally, interception leaves little or no trace. This imparted a new significance to encryption. It was the banking sector which first regularly used encryption to protect communications in the new area of electronic money transfers. The growing internationalisation of the economy led to communications in this field, too, being at least partly protected by cryptography. The widespread introduction of completely unprotected communications through the Internet also increased the need for private individuals to protect their messages from interception.

In the context of this report, then, the question arises as to whether there are cheap, legal, sufficiently secure and user-friendly methods of encrypting communications which can protect the individual against interception.

11.1.2. How encryption works

The principle of encryption is to convert a plain text into an encrypted text in such a way that it has either no meaning or a different meaning from the original, but can be converted back to the original by those in the know. For example, a meaningful sequence of letters can be transformed into a meaningless sequence which no outsider understands.

This is done according to a given method (encryption algorithm) based on the transposition and/or the substitution of letters. **The encryption method** (algorithm) is not nowadays kept

[244] There is evidence of this even in antiquity, e.g. the use of the *skytale* or cipher rod by the Spartans in the 5th century BC.

secret. On the contrary, a worldwide invitation to tender was recently issued for a new global encryption standard for use in industry. The same was done for the creation of a specific encryption algorithm as hardware in a machine (e.g. an encrypted fax machine).

What is **really secret** is the **key to the code.** This can be best explained by analogy. It is generally public knowledge how door locks work, not least because patents are held on them. Individual doors are protected by the fact that several different keys can exist for a particular type of lock. The same goes for the encryption of information: **many different** messages may be protected using individual keys, **kept secret** by those involved, on the basis of **one publicly known encryption method** (algorithm).

To explain these terms, we may use the example of the 'Caesarean encryption'. Julius Caesar encrypted messages simply by replacing each letter with the letter three places further on in the alphabet (A became D, B became E, etc.). The word **ECHELON** would thus become **HFKHORQ.** The **encryption algorithm** thus consists of the **shifting of letters** within the alphabet, and the **key** in this particular case is the instruction to move the letters **three places in the alphabet.** Both encryption and decryption are done in the same way: by moving letters three places: a symmetrical process. Nowadays this type of process would not provide protection for as much as a second!

A good encryption system may perfectly well be publicly known and still be regarded as secure. For this purpose, however, the number of possible keys needs to be so large that it is not possible to try all the keys (known as a **brute force attack**) in a reasonable time, even using computers. However, a large number of possible keys does not necessarily imply secure encryption if the method results in an encrypted text which gives clues to its decryption (e.g. the frequency of particular letters)[245]. Caesarean encryption is thus an insecure system for both reasons. Because it uses simple substitution, the varying frequency of letters in a language means that the procedure can quickly be cracked; moreover, since there are only 26 letters in the alphabet, there are only 25 possible letter shifts and thus only 25 possible keys. In this case, then, the codebreaker could very quickly find the key by trying all the possibilities and decipher the text.

We will now consider what a secure system should look like.

11.2. Security of encryption systems

11.2.1. Meaning of 'security' in encryption: general observations

If an encryption system is required to be 'secure', this may mean one of two things. Either it may be essential – and susceptible of mathematical proof – that the message is impossible to decipher without the key. Or it may be sufficient for the code to be unbreakable at the present state of technology and thus in all probability to meet the security requirement for far longer than the 'critical' period during which the message needs to be kept secret.

[245] *Otto Leiberich*, 'Vom diplomatischen Code zur Falltürfunktion – Hundert Jahre Kryptographie in Deutschland' [From diplomatic code to trap-door function – a hundred years of cryptography in Germany], *Spektrum der Wissenschaft* June 1999, 26 et seq.

11.2.2. Absolute security: the one-time pad

At present the only absolutely secure method is the one-time pad. This system was developed towards the end of the First World War[246], but was also used later for the telex hot-line between Moscow and Washington. The concept consists of a key comprising a non-repeating row of completely random letters. Both sender and recipient encrypt using these rows, and destroy the key as soon as it has been used once. Since there is no internal order within the key, it is impossible for a cryptoanalyst to break the code. This can be mathematically proven.[247]

The drawback to this process is that it is not easy to generate large numbers of these random keys[248], and that it is difficult and impractical to find a secure means of distributing the key. In normal business transactions, therefore, this method is not used.

11.2.3. Relative security at the present state of technology

11.2.3.1. The use of decryption and encryption machines

Even before the invention of the one-time pad, cryptographic processes were developed which could generate a large number of keys and thus produce coded texts which contained as few regularities in the text as possible and thus few starting-points for codebreaking. In order to make these methods sufficiently fast for practical application, machines were developed for encryption and decryption. The most spectacular of these was probably Enigma[249], used by Germany in the Second World War. The small army of decryption experts working at Bletchley Park in England succeeded in cracking the Enigma code by means of special machines known as 'bombs'. Both the Enigma machine and the 'bombs' were mechanical in operation.

11.2.3.2. Use of computers in cryptography

The invention of the computer represented a breakthrough in cryptography, since its power made it possible to use increasingly complex systems. Even though it did not alter the basic principles of encryption, a number of changes took place. Firstly, the level of potential complexity of the encryption system was multiplied, since it was no longer subject to the constraints of what was mechanically feasible, and, secondly, the speed of the encryption process rose drastically.

In computers, information is processed digitally using binary numbers. This means that the information is expressed by the sequence of two signals, 0 and 1. In physical terms 1 corresponds to an electric current or magnetic field ('light on'), while 0 means the absence of

[246] It was introduced by Major *Joseph Mauborgne*, head of the cryptographic research division of the American army; Simon Singh, The Code Book (1999), Carl Hanser Verlag 151.
[247] *Simon Singh*, The Code Book (1999), Carl Hanser Verlag 151 et seq.
[248] *Reinhard Wobst*, *Abenteuer Kryptologie*[2], Adison-Wesley (1998), 60.
[249] Enigma was developed by Arthur Scherbius and patented in 1928. It was a little like a typewriter, as it had a keyboard on which the plain text was keyed in. By means of a peg-board and rotating drums the text was encoded in accordance with given rules and decoded at the other end on the same machine using code books.

current or magnetic field ('light off'). ASCII[250] standardisation now prevails, whereby each letter is represented by a seven-figure combination of 0 and 1.[251] A text therefore appears as a sheet of 0s and 1s, and instead of letters it is numbers that are encrypted.

Both transposition and substitution can be used in this process. Substitution may, for example, take place by the addition of a key in the form of any row of numbers. According to the rules of binary mathematics the sum of two equal figures is zero (0+0=0 and 1+1=0) while the sum of two different figures is 1 (0+1=1). The new, encrypted row of figures arising from the addition of the key is thus a binary sequence which can either be further digitally processed or made readable again by subtracting the added key.

The use of computers made it possible to generate coded texts, using powerful encryption algorithms, which offer practically no starting-points for codebreakers. Decryption now entails trying all possible keys. The longer the key, the more likely it is that this attempt will be thwarted, even using very powerful computers, by the time it would take. There are therefore usable methods which may be regarded as secure at the present state of technology.

11.2.4. Standardisation and the deliberate restriction of security

As computers became more widely available in the 1970s, the need for the standardisation of encryption systems grow ever more urgent, since only in this way could firms communicate securely with business partners without incurring disproportionate costs. The first moves were made in the USA.

Powerful encryption systems can also be used for unlawful purposes or by potential military opponents; they may also make electronic espionage difficult or impossible. For that reason, the NSA urged that firms should be offered a sufficiently secure encryption standard, but one which the NSA itself could decrypt, by virtue of its exceptional technical capabilities. With that aim in mind, the length of the key was restricted to 56 bits. This reduces the number of possible keys to 100 000 000 000 000 000[252]. On 23 November 1976 Horst Feistel's so-called Lucifer key was officially adopted in its **56-bit version** under the name Data Encryption Standard (DES) and for the next 25 years represented the official US encryption standard[253]. This standard was also adopted in Europe and Japan, in particular in the banking sector. Media claims to the contrary, the DES algorithm has not yet been broken, but hardware now exists which is powerful enough to try all possible keys (brute force attack). In contrast, Triple DES, which has a 112-bit key, is still regarded as secure. The successor to DES, the Advanced Encryption Standard (AES), is a European process[254] which was developed under the name Rijndael in Louvain, Belgium. **It is fast and is regarded as secure, since it incorporates no key-length restriction.** The reason for this lies in a change in US policy on cryptography.

---

[250] American Standard Code for Information Exchange.
[251] A= 1000001, B= 1000010, C=1000011, D=1000100, E= 1000101, etc.
[252] In binary terms, this number consists of 56 zeros and ones. See Singh, The Code Book, Carl Hanser Verlag (1999), 303.
[253] *Simon Singh*, The Code Book, Carl Hanser Verlag (1999), 302 et seq.
[254] It was created by two Belgian cryptographers working at the Catholic University of Louvain, *Joan Daemen* and *Vincent Rijmen*.

Standardisation makes it much easier for firms to employ encryption. What remained, however, was the problem of key exchange.

11.3. The problem of the secure distribution/handover of keys

11.3.1. Asymmetric encryption: the public-key process

As long as a system works with a key which is employed both for encryption and decryption (symmetric encryption), it is difficult to use with **large numbers** of communication partners. The key must be handed over to every new communication partner **in advance** in such a way that no third party gains access to it. This is difficult for firms in practical terms, and feasible for private individuals only in rare cases.

Asymmetric encryption offers a solution to this problem: two different keys are used for encryption and decryption. The message is encrypted using a key which may perfectly well be in the public domain, the so-called **public key**. However, the process works only in one direction, with the result that decryption is no longer possible using the public key. For that reason, anybody who wishes to receive an encrypted message may send a communication partner via an unsecured route the public key required to encrypt the message. The received message is then decrypted using a different key, the **private key**, which is kept secret and which is not forwarded to communication partners[255]. The process can best be understood on the basis of a comparison with a padlock: anyone can snap a padlock together and, by so doing, secure a trunk; the padlock can only be opened, however, by a person with the right key[256]. Although the public and private keys are linked, the private key cannot be calculated on the basis of the public key.

Ron Rivest, Adi Shamir and Leonard Adleman invented an asymmetric encryption process which has been named after them (RSA process). In a one-way (trapdoor) function the result of the multiplication of two very large prime numbers is used as a component of the public key. The text is then encrypted using that key. Decryption is dependent on knowledge of the two prime numbers employed. However, there is no known mathematical process by means of which the large integers resulting from the multiplication of two prime numbers can be factored in such a way as to determine what those prime numbers were. At present, all possible combinations must be tried systematically. Given the present state of mathematical knowledge, therefore, the process is secure, provided that sufficiently large prime numbers are chosen. The only risk is that at some stage a brilliant mathematician will discover a quicker factoring method. Thus far, however, even the best efforts have proved fruitless[257]. Many people even claim that the problem is insoluble, but this theory has not yet been proved[258].

By comparison with symmetric processes (e.g. DES), however, public-key encryption requires much more PC calculation time or the use of rapid, large-scale computers.

---

[255] The idea of asymmetric encryption using the public-key process was devised by *Whitfield Diffie* and *Martin Hellmann.*
[256] *Simon Singh*, The Code Book, Carl Hanser Verlag (1999), 327.
[257] *Johannes Buchmann*, Factoring large integers, Spektrum der Wissenschaft 2, 1999, 6 et seq.
[258] *Simon Singh*, The Code Book, Carl Hanser Verlag (1999), 335 et seq.

11.3.2. Public-key encryption for private individuals

In order to make the public-key process generally accessible, Phil Zimmermann came up with the idea of linking the public-key process, which involves a great deal of calculation, with a faster symmetric process. The message itself should be encrypted using an asymmetric process, the IDEA process developed in Zurich, but the key to the symmetric encryption would be exchanged at the same time, as in the public-key process. Zimmermann developed a user-friendly programme (Pretty Good Privacy) which created the requisite key and carried out the encryption at the push of a button (or the click of a mouse). The programme was placed on the Internet, from where anyone could download it. PGP was ultimately bought by the US firm NAI, but is still made available to private individuals free of charge[259]. The source text for the earlier versions has been published, so it can be assumed that no backdoors have been incorporated. Unfortunately, the source texts for the newest version, PGP 7, which is characterised by an exceptionally user-friendly graphic interface, are no longer published.

There is, however, a further implementation of the Open PGP Standard: GnuPG. GnuPG offers the same encryption methods as PGP, and is also compatible with PGP. However, it is freeware, its source code is known and any individual can use it and pass it on. The Federal German Ministry for Economic Affairs and Technology has promoted the porting of GnuPG on Windows and the development of a graphic interface; unfortunately, however, these functions have not yet been fully developed. According to the information available to your rapporteur, work is continuing.

There are also rival standards to OpenPGP, such as S/MIME, which are supported by many e-mail programmes. Here, your rapporteur has no information on free implementation.

11.3.3. Future processes

In the future quantum cryptography may open up new prospects for secure key exchange. It would ensure that the interception of a key exchange could not pass unnoticed. If polarised photons are transmitted, the fact of their polarisation cannot be established without altering that polarisation. Eavesdroppers on the line could thus be detected with 100% certainty. Only those keys which had not been intercepted would then be used. In experiments, transmission over 48 km via fibreoptic cable and over 500 m through the air has already been achieved[260].

11.4. Security of encryption products

In the discussion on the actual level of security of encryption processes the accusation has repeatedly been made that American products contain backdoors. For example, Excel made headlines here in Europe when it was suggested that in the European version of its programme half the key is revealed in the file header. Microsoft also gained media attention when a hacker claimed to have discovered an 'NSA key' hidden in the programme, a claim which was of course strongly denied by Microsoft. Since Microsoft has not revealed its source code, any assessment amounts to pure speculation. At all events, the earlier versions of PGP and

[259] Information on the software can be found at www.pgpi.com.
[260] On quantum cryptology, see *Reinhard Wobst*, Abenteuer Kryptographie[2], Adison-Wesley (1998), 224 et seq.

GnuPG can be said with a great degree of certainty not to contain such a backdoor, since their source text has been disclosed.

11.5. Encryption in conflict with state interests

11.5.1. Attempts to restrict encryption

Many states initially ban the use of encryption software or cryptographic equipment and make exceptions only subject to prior authorisation. The states concerned are not just dictatorships such as China, Iran or Iraq. Democratic states have also imposed legal restrictions on the use or purchase of encryption programmes or equipment. It would appear that communications are to be protected against being read by unauthorised private individuals, but that the state should retain the possibility of intercepting such communications, if necessary on the basis of specific legal provisions. The authorities' loss of technical superiority is thus made good by means of legal bans. For example, until recently France imposed a general ban on the use of cryptography, granting authorisations only in individual cases. A few years ago in Germany a debate arose concerning restrictions on encryption and the compulsory submission of a key to the authorities. In the past, the USA has taken a different course, imposing restrictions on key length.

11.5.2. The significance of secure encryption for e-commerce

By now, these attempts should have been shown, once and for all, to be futile. The state's interest in having access to encryption processes and thus to the plain texts does not only stand in opposition to the right to privacy, but also to entrenched economic interests. E-commerce and electronic banking are dependent on secure communications via the Internet. If this cannot be guaranteed, these techniques are doomed to failure, owing to a lack of customer confidence. This link explains the about-turn in US or French policy on cryptography.

It should be pointed out here that there are two reasons why e-commerce needs secure encryption processes: not only in order to encrypt messages, but also to prove beyond doubt the identity of business partners. The electronic signature procedure can be carried out using a reversal of the public-key process: the private key is used to encrypt the signature, and the public key to decrypt it. This form of encryption confirms the authenticity of the signature. Through the use of the public key, any individual can convince another of his or her genuineness, but he or she cannot imitate the signature itself. This function is also built into PGP as an additional user-friendly feature.

11.5.3. Problems for business travellers

In some states business travellers are prohibited from using encryption programmes on the laptop computers they carry with them, ruling out any protection of communications with their own firm or the data stored on those computers.

11.6. Practical issues in connection with encryption

When answering the question of what persons, and under what circumstances, should be advised to employ encryption, a distinction must be drawn between private individuals and firms.

As far as private individuals are concerned, it must be clearly stated that the encryption of fax and telephone messages using a cryptotelephone or cypherfax is not really a workable option, not only because the cost of purchasing such equipment is relatively high, but also because their use presupposes that the interlocutor also has such equipment available, which is doubtless only very rarely the case.

In contrast, e-mails can and should be encrypted by everyone. The oft-repeated claim that a person has no secrets and thus has no need to encrypt messages must be countered by pointing out that written messages are not normally sent on postcards. However, an unencrypted e-mail is nothing other than a letter without an envelope. The encryption of e-mails is secure and relatively straightforward and user-friendly systems, such as PGP/GnuPG, are already available, even free of charge, to private individuals on the Internet. Unfortunately, they are not yet sufficiently widely distributed. The public authorities should set a good example and themselves employ encryption as a standard practice in order to demystify the process.

As far as firms are concerned, they should take strict measures to ensure that sensitive information is only transmitted via secure media. This may seem obvious, and no doubt is for large undertakings, but in small- and medium-sized firms in particular internal information is often transmitted via unencrypted e-mails, because awareness of the problem is not sufficiently well developed. In this connection, it can only be hoped that industry associations and chambers of commerce will step up their efforts to increase that awareness. Admittedly, the encryption of e-mails is only one security aspect amongst many, and serves no purpose if the information is made available to others prior to encryption. The implication is that the entire working environment must be protected, thereby guaranteeing the security of a firm's premises, and checks must be carried out on persons entering offices and accessing computers. In addition, unauthorised access to information via the firm's network must be prevented by means of the introduction of corresponding firewalls. Here, particular dangers are posed by the linking of the firm's internal network and the Internet. If security is to be taken seriously, only those operating systems should be used whose source code has been published and checked, since only then can it be determined with certainty what happens to the data. Firms are thus faced with a wide variety of tasks in the security sphere. Many businesses have already been set up to provide security advice and arrangements at affordable prices, and the supply of such services is expanding steadily in line with demand. In addition, however, it must be hoped that industry associations and chambers of commerce take up this issue, particularly in order to draw the attention of small firms to the problem of security and to support efforts to devise and implement comprehensive protection arrangements.

12. The EU's external relations and intelligence gathering

12.1. Introduction

With the adoption of the Maastricht Treaty in 1991, the Common Foreign and Security Policy (CFSP) was established in its most elementary form as a new policy instrument for the European Union. Six years later the Amsterdam Treaty gave further structure to the CFSP and created the possibility for common defence initiatives within the European Union, whilst maintaining the existing alliances. On the basis of the Amsterdam Treaty and with the experiences in Kosovo in mind, the Helsinki European Council of December 1999 launched the European Security and Defence Initiative. This initiative aims at the creation of a multinational force of between 50 000 and 60 000 troops by the second half of 2003. The existence of such a multinational force will make the development of an autonomous intelligence capacity inevitable. The simple integration of the existing WEU intelligence capacity will be insufficient for this purpose. Further cooperation between the intelligence agencies of the Member States, well beyond the existing forms of cooperation, cannot be avoided.

However, the further development of the CFSP is not the only factor leading to closer cooperation among the Union's intelligence services. Further economic integration within the European Union will likewise necessitate a more intensive cooperation in the field of intelligence collection. A united European economic policy implies a united perception of economic reality in the world outside the European Union. A united position in trade negotiations within the WTO or with third countries calls for joint protection of the negotiating position. Strong European industries need joint protection against economic espionage from outside the European Union.

It must finally be emphasised that further development of the Union's second pillar and the Union's activities in the field of Justice and Home Affairs will inevitably also lead to further cooperation between intelligence services. In particular, the joint fight against terrorism, illegal trade in arms, trafficking of human beings, and money laundering cannot take place without intensive cooperation between intelligence services.

12.2. Scope for cooperation within the EU

12.2.1. Existing cooperation[261]

Although there is a long tradition within the intelligence services of only trusting the information they collect themselves and maybe even of distrust between the different intelligence services within the European Union, cooperation between services is already gradually increasing. Frequent contacts do exist within the framework of NATO, the WEU and within the European Union. And whereas, within the framework of NATO, the intelligence services are still heavily dependent on the far more sophisticated contributions from the United States, the establishment of the WEU satellite centre in Torrejon (Spain) and

[261] *Charles Grant,* Intimate relations. Can Britain play a leading role in European defence - and keep its special links to US intelligence? 4.2000, Centre for European Reform

the creation of an intelligence section attached to the WEU headquarters have contributed to more autonomous European action in this field.

12.2.2. Advantages of a joint European intelligence policy

In addition to these developments already taking place, it must be emphasised that there are objective advantages to a joint European intelligence policy. These advantages may be described as follows.

12.2.2.1. Practical advantages

First of all there is simply too much classified and unclassified material available to be collected, analysed, and evaluated by any single agency or under any single bilateral agreement in Western Europe. The demands on intelligence services range from defence intelligence, through intelligence on third states' internal and international economic policies, to intelligence in support of the fight against organised crime and drug trafficking. Even if cooperation existed only on the most basic level, i.e. as regards the collection of open-source intelligence (OSINT), the results of this cooperation would already be of great importance for the European Union's policies.

12.2.2.2. Budgetary advantages

In the recent past budgets for intelligence collection have been cut and, in some cases, are still being reduced. At the same time, the demand for information and therefore intelligence has grown. These reduced budgets do not only make this cooperation desirable but, in the long run, also profitable. In particular, in the case of establishing and maintaining technical facilities, joint operations are of interest when money is scarce but also when it comes to evaluating the collected information. Further cooperation will increase the effectiveness of intelligence collection.

12.2.2.3. Political advantages

In principle, collected intelligence is used to give governments the possibility of better and better-founded decision-making. Further political and economic integration in the European Union demands that intelligence should be available at European level and should also be based on more than one single source.

12.2.3. Concluding remarks

These objective advantages merely illustrate the growing importance of cooperation within the European Union. In the past nation states used to guarantee their own external security, internal order, national prosperity and cultural identity. Today, the European Union is in many fields in the process of taking up a role at least complementary to that of the nation state. It is inconceivable that the intelligence services will be the last and only area not affected by the process of European integration.

12.3. Cooperation beyond EU level

Following the Second World War cooperation in the field of intelligence collection did not at first take place at European level, but far more at transatlantic level. It has already been shown that very close relations in the field of intelligence gathering were established between the United Kingdom and the United States. But also in the field of defence intelligence within the framework of NATO and beyond, the United States was and still is the absolutely dominant partner. The major question therefore is this: will growing European cooperation in the field of intelligence gathering seriously disrupt relations with the United States, or might it lead to a strengthening of those relations? How will EU/US relations develop under the new Bush Administration? And, in particular, how will the special relationship between the United States and the United Kingdom be maintained in this framework?

Some take the view that there need not be a contradiction between the British/US special relationship and the further development of the CFSP. Others believe that intelligence gathering may be precisely the issue which forces the United Kingdom to decide whether its destiny is European or transatlantic. Britain's intimate links with the US (and with the other partners in the UKUSA Agreement) may make it more difficult for other EU states to share intelligence amongst themselves – because the United Kingdom may be less interested in intra-European sharing, and because its EU partners may trust the United Kingdom less. Equally, if the US believes that the United Kingdom has developed special links with its EU partners, and that this is part of a European special agreement, the US may become reluctant to continue sharing its intelligence with the United Kingdom. Closer EU cooperation in the field of intelligence may therefore constitute a serious test of the European ambitions of the United Kingdom and of the EU's capacity for integration.

In the present circumstances it is, however, highly unlikely that even extremely rapid progress in cooperation among the European partners can, in the short and even in the longer term, offset the technological advantage enjoyed by the United States. The European Union will not be able to establish a sophisticated network of SIGINT satellites, imaging satellites and ground stations. The European Union will not be able to develop, in the short term, the highly sophisticated network of computers required for the selection and evaluation of the collected material. The European Union will not be prepared to make available the budgetary resources needed to develop a true alternative to the intelligence efforts of the United States. Purely from a technological and budgetary viewpoint, therefore, it will be in the interests of the European Union to maintain a close relationship with the United States in the field of intelligence collection. But also from a more political point of view, it will be important to maintain and, where necessary, strengthen relationships with the United States, in particular in the context of the joint fight against organised crime, terrorism, drugs and arms trafficking and money laundering. Joint intelligence operations are necessary to support a joint fight. Joint peacekeeping actions, such as in former Yugoslavia, demand a greater European contribution in all areas.

On the other hand, growing European awareness should be accompanied by greater European responsibility. The European Union should become a more equal partner, not only in the economic field, but also in the field of defence and therefore in the field of intelligence collection. A more autonomous European intelligence capacity should therefore not be seen as weakening transatlantic relations, but should be used to strengthen them by establishing the European Union as a more equal and more capable partner. At the same time, the European Union must make independent efforts to protect its economy and its industry against illegal

and unwanted threats such as economic espionage, cyber-crime, and terrorist attacks. However, transatlantic understanding is necessary in the field of industrial espionage. The European Union and the United States should agree on a set of rules laying down what is and what is not allowed in this area. With a view to strengthening transatlantic cooperation in this field, a joint initiative could be undertaken at WTO level using that organisation's mechanisms to safeguard fair economic development worldwide.

12.4. Final remarks

Although the issue of the protection of European citizens' privacy must remain fundamental, the further development of a joint European Union intelligence capacity should be considered necessary and inevitable. Cooperation with third countries, and in particular the United States, should be maintained and, very possibly, strengthened. This does not necessarily mean that European SIGINT activities should automatically be integrated in an independent European Union ECHELON system, or that the European Union should become a full partner in the present UKUSA Agreement. However, the development of proper European responsibility in the field of intelligence collection must be actively considered. An integrated European intelligence capacity demands, at the same time, a system of European political control over the activities of these agencies. Decisions will have to be taken on the procedure for assessing intelligence and for taking the political decisions which result from an analysis of intelligence reports. The lack of such a system of political control, and therefore of political awareness and responsibility for the process of intelligence collection, would be detrimental to the process of European integration.

13. Conclusions and recommendations

13.1. Conclusions

The existence of a global system for intercepting private and commercial communications (the ECHELON interception system)

That a global system for intercepting communications exists, operating by means of cooperation proportionate to their capabilities among the USA, the UK, Canada, Australia and New Zealand under the UKUSA Agreement, is no longer in doubt. It may be assumed, in view of the evidence and the consistent pattern of statements from a very wide range of individuals and organisations, including American sources, that the system or parts of it were, at least for some time, code-named ECHELON. What is important is that its purpose is to intercept private and commercial communications, and not military communications.

Analysis has revealed that the technical capabilities of the system are probably not nearly as extensive as some sections of the media had assumed. Nevertheless, it is worrying that many senior Community figures, in particular European Commissioners, who gave evidence to the Temporary Committee, claimed to be unaware of this phenomenon.

The limits of the interception system

The surveillance system depends, in particular, upon worldwide interception of satellite communications. However, in areas characterised by a high volume of traffic only a very small proportion of those communications are transmitted by satellite. This means that the majority of communications cannot be intercepted by earth stations, but only by tapping cables and intercepting radio signals. However, inquiries have shown that the UKUSA states have access to only a very limited proportion of cable and radio communications, and, owing to the large numbers of personnel required, can analyse only an even smaller proportion of those communications. However extensive the resources and capabilities for the interception of communications may be, the extremely high volume of traffic makes exhaustive, detailed monitoring of all communications impossible in practice.

The possible existence of other interception systems

Since intercepting communications is a method of spying commonly employed by intelligence services, other states might also operate similar systems, provided that they have the required funds and the right locations. France, thanks to its overseas territories, is the only EU Member State which is geographically and technically capable of operating a global interception system by itself. There is ample evidence that Russia also operates such a system.

Compatibility with EU law

As regards the question of the compatibility of a system of the ECHELON type with EU law, it is necessary to distinguish between two scenarios. If a system is used purely for intelligence purposes, there is no violation of EU law, since operations in the interests of state security are not subject to the EC Treaty, but would fall under Title V of the Treaty on European Union

(CFSP), although at present that title lays down no provisions on the subject, so no criteria are available. If, on the other hand, the system is misused for the purposes of gathering competitive intelligence, such action is at odds with the Member States' duty of loyalty and with the concept of a common market based on free competition. If a Member State participates in such a system, it violates EC law.
At its meeting of 30 March 2000 the Council made clear that it cannot agree to the creation or existence of an interception system which does not comply with the rules laid down in the laws of the Member States and which breaches the fundamental principles designed to safeguard human dignity.

Compatibility with the fundamental right to respect for private life (Article 8 of the ECHR)

Any interception of communications represents serious interference with an individual's exercise of the right to privacy. Article 8 of the ECHR, which guarantees respect for private life, permits interference with the exercise of that right only in the interests of national security, in so far as this is in accordance with domestic law and the provisions in question are generally accessible and lay down under what circumstances, and subject to what conditions, the state may undertake such interference. Interference must be proportionate: thus competing interests need to be weighed up and it is not enough that the interference should merely be useful or desirable.

An intelligence system which intercepted communications permanently and at random would be in violation of the principle of proportionality and would therefore not be compatible with the ECHR. It would also constitute a violation of the ECHR if the rules governing the surveillance of communications lacked a legal basis, if the rules were not generally accessible or if they were so formulated that their implications for the individual were unforeseeable. Since most of the rules governing the activities of US intelligence services abroad are classified, compliance with the principle of proportionality is at least doubtful and breaches of the principles of accessibility and foreseeability laid down by the European Court of Human Rights probably occur. Although the USA is not itself an ECHR contracting party, the Member States must nevertheless act in a manner consistent with the ECHR. The Member States cannot circumvent the requirements imposed on them by the ECHR by allowing other countries' intelligence services, which are subject to less stringent legal provisions, to work on their territory, since otherwise the principle of legality, with its twin components of accessibility and foreseeability, would become a dead letter and the case law of the European Court of Human Rights would be deprived of its substance.

In addition, the lawful operations of intelligence services are consistent with fundamental rights only if adequate arrangements exist for monitoring them, in order to counterbalance the risks inherent in secret activities performed by a part of the administrative apparatus. As the European Court of Human Rights has expressly stressed the importance of an efficient system for monitoring intelligence operations, there are grounds for concern in the fact that some Member States do not have parliamentary monitoring bodies of their own responsible for scrutinising the secret services.

Are EU citizens adequately protected against intelligence services?

As the protection enjoyed by EU citizens depends on the legal situation in the individual Member States, which varies very substantially, and since in some cases parliamentary monitoring bodies do not even exist, the degree of protection can hardly be said to be adequate. It is in the fundamental interests of European citizens that their national parliaments should have a specific, formally structured monitoring committee responsible for supervising and scrutinising the activities of the intelligence services. But even where monitoring bodies do exist, there is a strong temptation for them to concentrate more on the activities of domestic intelligence services, rather than those of foreign intelligence services, since as a rule it is only the former which affect their own citizens.

In the event of cooperation between intelligence services under the CFSP and between the security authorities in the spheres of justice and home affairs, the institutions must introduce adequate measures to protect European citizens.

Industrial espionage

Part of the remit of foreign intelligence services is to gather economic data, such as details of developments in individual sectors of the economy, trends on commodity markets, compliance with economic embargoes, observance of rules on supplying dual-use goods, etc. For these reasons, the firms concerned are often subject to surveillance. The US intelligence services do not merely gather general economic intelligence, but also intercept communications between firms, particularly where contracts are being awarded, and they justify this on the grounds of combating attempted bribery. Detailed interception poses the risk that information may be used as competitive intelligence, rather than combating corruption, even though the US and the United Kingdom state that they do not do so. However, the role of the Advocacy Center of the US Department of Commerce is still not totally clear and talks arranged with the Center with a view to clarifying the matter were cancelled. It should also be pointed out that an agreement on combating the bribery of officials, under which bribery is criminalised at international level, was adopted by the OECD in 1997, and this provides a further reason why individual cases of bribery cannot justify the interception of communications. At all events, it must be made clear that the situation becomes intolerable when intelligence services allow themselves to be used for purposes of gathering competitive intelligence by spying on foreign firms with the aim of securing a competitive advantage for firms in the home country. Although it is frequently maintained that the global interception system considered in this report has been used in this way, no such case has been substantiated.

The fact is that sensitive commercial data are mostly kept inside individual firms, so that competitive intelligence-gathering primarily involves efforts to obtain information through members of staff or through people planted in the firm for this purpose or else, more and more frequently, by hacking into internal computer networks. Only if sensitive data are transmitted externally by cable or radio (satellite) can a communications surveillance system be used for competitive intelligence-gathering. This applies systematically in the following three cases:
- in the case of firms which operate in three time zones, so that interim results are sent from Europe to America and on to Asia;
- in the case of videoconferencing within multinationals using VSAT or cable;

- if vital contracts are being negotiated on the spot (e.g. for the building of plants, the development of telecommunications infrastructure, the creation of new transport systems, etc.) and it is necessary to consult the company's head office.
Risk and security awareness in small and medium-sized firms is unfortunately often inadequate and the dangers of economic espionage and the interception of communications are often not recognised.
Since security awareness is likewise not always well developed in the European institutions (with the exception of the European Central Bank, the Council Directorate-General for External Relations and the Commission Directorate-General for External Relations), immediate action is therefore necessary.

Possible self-protection measures

Firms must secure the whole working environment and protect all communications channels which are used to send sensitive information. Sufficiently secure encryption systems exist at affordable prices on the European market. Private individuals should also be urged to encrypt e-mails: an unencrypted e-mail message is like a letter without an envelope. Relatively user-friendly systems exist on the Internet which are even made available for private use free of charge.

Cooperation among intelligence services within the EU

In December 1999 in Helsinki the European Council decided to develop more effective European military capabilities with a view to undertaking the full range of Petersberg tasks in support of the CFSP. In order to achieve this goal, by the year 2003 the Union was to be able to rapidly deploy units of about 50 000 – 60 000 troops which should be self-sustaining, including the necessary command, strategic reconnaissance and intelligence capabilities. The first steps towards such an autonomous intelligence capability have already been taken in the framework of the WEU and the standing Political and Security Committee. Cooperation among intelligence services within the EU seems essential on the grounds that, firstly, a common security policy which did not involve the secret services would not make sense and, secondly, it would have numerous professional, financial and political advantages. It would also accord better with the idea of the EU as a partner on an equal footing with the United States and could bring together all the Member States in a system which complied fully with the ECHR. The European Parliament would of course have to exercise appropriate monitoring. The European Parliament is in the process of implementing the Regulation (EC) No 1049/2001 on public access to European Parliament, Council and Commission documents by revising the provisions of its Rules of Procedure as regards access to sensitive documents.

13.2. Recommendations

Conclusion and amendment of international agreements on the protection of citizens and firms

1. The Secretary-General of the Council of Europe is called upon to submit to the Ministerial Committee a proposal to protect private life, as guaranteed in Article 8 of the ECHR, brought into line with modern communication and interception methods by means of an additional protocol or, together with the provisions governing data

protection, as part of a revision of the Convention on Data Protection, with the proviso that this should neither undermine the level of legal protection established by the European Court of Human Rights nor reduce the flexibility which is vital if future developments are to be taken into account.

2. The Member States of the European Union are called upon to establish a European platform consisting of representatives of the national bodies that are responsible for monitoring Member States' performance in complying with fundamental and citizens' rights in order to scrutinise the consistency of national laws on the intelligence services with the ECHR and the EU Charter of Fundamental Rights, to review the legal provisions guaranteeing postal and communications secrecy, and, in addition, to reach agreement on a recommendation to the Member States on a Code of Conduct to be drawn up which guarantees all European citizens, throughout the territory of the Member States, protection of privacy as defined in Article 7 of the Charter of Fundamental Rights of the European Union and which, moreover, guarantees that the activities of intelligence services are carried out in a manner consistent with fundamental rights, in keeping with the conditions set out in Chapter 8 of this report, and in particular Section 8.3.4., as derived from Article 8 of the ECHR.

3. The member countries of the Council of Europe are called upon to adopt an additional protocol which enables the European Communities to accede to the ECHR or to consider other measures designed to prevent disputes relating to case law arising between the European Court of Human Rights and the Court of Justice of the European Communities.

4. The Member States are called upon, at the next Intergovernmental Conference, to adopt the EU Charter of Fundamental Rights as a legally binding and enforceable act in order to raise the standard of protection for fundamental rights, particularly with regard to the protection of privacy. The EU institutions are called upon to comply with the fundamental rights laid down in the Charter in their respective areas of responsibility and activity.

5. The European Union and the USA are called upon to conclude an agreement on the basis of which each party applies to the other the rules governing the protection of privacy and the confidentiality of business communications which are valid for its own citizens and firms.

6. The Member States are called upon to conclude an agreement with third countries aimed at providing increased protection of privacy for EU citizens, under which all contracting states give a commitment, where one contracting state intercepts communications in another contracting state, to inform the latter of the planned actions.

7. The UN Secretary-General is called upon to instruct the competent committee to put forward proposals designed to bring Article 17 of the International Covenant on Civil and Political Rights, which guarantees the protection of privacy, into line with technical innovations.

8. The USA is called upon to sign the Additional Protocol to the International Covenant on Civil and Political Rights, so that complaints by individuals concerning breaches of the

Covenant by the USA can be submitted to the Human Rights Committee set up under the Covenant. The relevant US NGOs, in particular the ACLU (American Civil Liberties Union) and the EPIC (Electronic Privacy Information Center), are called upon to exert pressure on the US Administration to that end.

9. The Council and the Member States are strongly urged to establish as a matter of priority a system for the democratic monitoring and control of the autonomous European intelligence capability and other joint and coordinated intelligence activities at European level. The European Parliament should play an important role in this monitoring and control system.

National legislative measures to protect citizens and firms

10. The Member States are strongly urged to review their own legislation on the operations of the intelligence services to ensure that it is consistent with the fundamental rights laid down in the ECHR and in the case law of the European Court of Human Rights and, if necessary, to adopt appropriate legal provisions. They are called upon to afford all European citizens the same legal guarantees concerning the protection of privacy and the confidentiality of correspondence. Any of their laws which are discriminatory in terms of the surveillance powers granted to the secret services must be repealed.

11. The Member States are called upon to aspire to a common level of protection against intelligence operations and, to that end, to draw up a code of conduct based on the highest level of protection which exists in any Member State, since as a rule it is citizens of other states, and hence also of other Member States, that are affected by the operations of foreign intelligence services. A similar code of conduct should be negotiated with the USA.

12. The Member States are called upon to pool their communications interception resources with a view to enhancing the effectiveness of the CFSP in the areas of intelligence-gathering and the fight against terrorism, nuclear proliferation or international drug trafficking, in accordance with the provisions governing the protection of citizens' privacy and the confidentiality of business communications, and subject to monitoring by the European Parliament, the Council and the Commission.

Specific legal measures to combat industrial espionage

13. The Member States are called upon to consider to what extent industrial espionage and the payment of bribes as a way of securing contracts can be combated by means of European and international legal provisions and, in particular, whether WTO rules could be adopted which take account of the distortions of competition brought about by such practices, for example by rendering contracts obtained in this way null and void. The USA, Canada, Australia and New Zealand are called upon to join this initiative.

14. The Member States are called upon to give a binding undertaking neither to engage in industrial espionage, either directly or behind the front offered by a foreign power active on their territory, nor to allow a foreign power to carry out such espionage from their territory, thereby acting in accordance with the letter and spirit of the EC Treaty.

15. The Member States and the US Administration are called upon to start an open US-EU dialogue on economic intelligence-gathering.

16. The authorities of the United Kingdom are called upon to explain their role in the UK/USA alliance in connection with the existence of a system of the 'ECHELON' type and its use for the purposes of industrial espionage.

17. The Member States are called upon to ensure that their intelligence services are not misused for the purposes of obtaining competitive intelligence, since this would be at odds with the Member States' duty of loyalty and the concept of a common market based on free competition.

Measures concerning the implementation of the law and the monitoring of that implementation

18. The Member States are called upon to guarantee appropriate parliamentary and legal monitoring of their secret services. Those national parliaments which have no monitoring body responsible for scrutinising the activities of the intelligence services are called upon to set up such a body.

19. The monitoring bodies responsible for scrutinising the activities of the secret services are called upon, when exercising their monitoring powers, to attach great importance to the protection of privacy, regardless of whether the individuals concerned are their own nationals, other EU nationals or third-country nationals.

20. The Member States' intelligence services are called upon to accept data from other intelligence services only in cases where such data has been obtained in accordance with the conditions laid down by their own domestic law, as Member States cannot evade the obligations arising from the ECHR by using other intelligence services.

21. Germany and the United Kingdom are called upon to make the authorisation of further communications interception operations by US intelligence services on their territory conditional on their compliance with the ECHR, i.e. to stipulate that they should be consistent with the principle of proportionality, that their legal basis should be accessible and that the implications for individuals should be foreseeable, and to introduce corresponding, effective monitoring measures, since they are responsible for ensuring that intelligence operations authorised or even merely tolerated on their territory respect human rights.

Measures to encourage self-protection by citizens and firms

22. The Commission and Member States are called upon to inform their citizens and firms about the possibility of their international communications being intercepted. This information must be combined with practical assistance in developing and implementing comprehensive protection measures, not least as regards IT security.

23. The Commission, the Council and the Member States are called upon to develop and implement an effective and active policy for security in the information society. As part of that policy, specific attention should be given to increasing the awareness of all users

of modern communication systems of the need to protect confidential information. A Europe-wide, coordinated network of agencies capable of providing practical assistance in designing and implementing comprehensive protection strategies must be established.

24. The Commission and Member States are urged to devise appropriate measures to promote, develop and manufacture European encryption technology and software and above all to support projects aimed at developing user-friendly open-source encryption software.

25. The Commission and Member States are called upon to promote software projects whose source text is made public (open-source software), as this is the only way of guaranteeing that no backdoors are built into programmes. The Commission is called upon to lay down a standard for the level of security of e-mail software packages, placing those packages whose source code has not been made public in the 'least reliable' category.

26. The European institutions and the public administrations of the Member States are called upon systematically to encrypt e-mails, so that ultimately encryption becomes the norm.

Measures to improve security in the institutions

27. The Community institutions and the public administrations of the Member States are called upon to provide training for their staff and make their staff familiar with new encryption technologies and techniques by means of the necessary practical training and courses.

28. The Commission is instructed to have a security analysis carried out which will show what needs to be protected, and to have a protection strategy drawn up.

29. The Commission is called upon to update its encryption system in line with the latest developments, given that modernisation is urgently needed, and calls on the budgetary authority (the Council together with Parliament) to provide the necessary funding.

30. The competent committee is requested to draw up an own-initiative report on security and the protection of secrecy in the European institutions.

31. The Commission is called upon to ensure that data is protected in its own IT systems and to step up the protection of secrecy in relation to documents not accessible to the public.

32. The Commission and the Member States are called upon to invest in new technologies in the field of decryption and encryption techniques as part of the Sixth Research Framework Programme.

Other measures

33. Firms are called upon to cooperate more closely with counter-espionage services, and particularly to inform them of attacks from outside for the purposes of industrial espionage, in order to improve the services' efficiency.

34. The Commission is called upon to put forward a proposal to establish, in close cooperation with industry and the Member States, a Europe-wide, coordinated network of advisory centres - in particular in those Member States where such centres do not yet exist - to deal with issues relating to the security of the information held by firms, with the twin task of increasing awareness of the problem and providing practical assistance.

35. The Commission is called upon to pay particular attention to the position of the applicant countries; if their lack of technological independence prevents them from implementing the requisite protective measures they should be given support.

36. The European Parliament is called upon to hold an international congress on the protection of privacy against telecommunications surveillance in order to provide NGOs from Europe, the USA and other countries with a forum for discussion of the cross-border and international aspects of the problem and coordination of areas of activity and action.

EUROPEAN PARLIAMENT

1999 *2004*

Session document

FINAL
A5-0264/2001
Part 2

11 July 2001

REPORT

on the existence of a global system for the interception of private and commercial communications (ECHELON interception system) (2001/2098 (INI))

Part 2: Minority Opinions
Annexes

Temporary Committee on the ECHELON Interception System

Rapporteur: Gerhard Schmid

CONTENTS

Page

MINORITY OPINION by Giuseppe Di Lello, Pernille Frahm and Alain Krivine 4
MINORITY OPINION by Patricia McKenna and Ilka Schröder 5
MINORITY OPINION by Jean-Charles Marchiani 6
MINORITY OPINION by Maurizio Turco 7
Annex I: List of the experts who provided the committee with information 8
Annex II: Bibliography ..... 11 Annex III: De
communications for the purpose of criminal prosecution 17

1. Preliminary remarks 17

2. Distinction between the interception of communications for the purpose of criminal prosecution and for the purpose of intelligence gathering 17

3. Activities in the EU in the field of interception of communications for the purpose of criminal prosecution 18

3.1. General remarks 18

3.2. Restriction of EU powers and responsibilities to technical arrangements 18

3.3. Activities and legal acts in the field of interception of telecommunications 19

4. Definitions and explanations concerning further international activities in the field of interception of telecommunications 21

Annex IV: 23

MINORITY OPINION by Giuseppe Di Lello, Pernille Frahm and Alain Krivine

The report by the Temporary Committee confirms the existence of the Echelon interception system which is administered by various countries, including the United Kingdom, a Member State of the European Union, with the cooperation of Germany.

An interception system of this nature, which does not differentiate between communications, data and documents, infringes the fundamental right to privacy guaranteed by Article 8 of the European Convention on Human Rights and Article 6 of the Treaty on European Union.

The system therefore flagrantly infringes the freedoms enjoyed by European citizens, the logic of the free market and the security of the Union. Whatever our support for or opposition to that logic and those treaties may be, such infringements are unacceptable.

In its conclusions, the report ought to have called on the United Kingdom to dissociate itself from the Echelon system and on Germany to close the listening post located on its soil. It is a matter of regret that the European Union is more preoccupied with industrial espionage than with individual monitoring.

MINORITY OPINION by Patricia McKenna and Ilka Schröder

This report makes an important point in emphasising that Echelon does exist, but it stops short of drawing political conclusions. It is hypocritical for the European Parliament to criticise the Echelon interception practice while taking part in plans to establish a European Secret Service.

No effective public control mechanism of secret services and their undemocratic practices exists globally. It is in the nature of secret services that they cannot be controlled. They must therefore be abolished. This report serves to legitimise a European Secret Service which will infringe fundamental rights - just as Echelon does.

For the majority in Parliament, the focus is industry, where profit interests are supposedly threatened by industrial espionage. However, the vital issue is that no one can communicate in confidence over distances any more. Political espionage is a much greater threat than economic espionage.

This report constantly plays down these dangers of Echelon, while it remains silent about plans to introduce the ENFOPOL interception system in the EU. Every society must take a fundamental decision whether or not to live under permanent control. By adopting this report, the European Parliament shows that it is not concerned about protecting human rights and citizens' liberties.

MINORITY OPINION by Jean-Charles Marchiani

The UEN Group was not surprised at the outcome of the vote on Mr Schmid's report which, originally, was supposed to concern itself with the Echelon espionage system set up by certain English-speaking countries.

From the outset, a majority within Parliament had clearly indicated its intentions, preferring to set up this temporary committee rather than a full-blown committee of inquiry. Accordingly, it had nothing else to fear from proceedings where the rapporteur's ability to create regular diversions was in no way threatened by a band of malcontents whose motives were too disparate.

Our message is crystal-clear: Mr Schmid's efforts have been unable to conceal either the existence of the Echelon system or the active or passive involvement of several Member States.

That has resulted in a serious breach of the principles underlying the treaties which ought to have led to sanctions being imposed or, at the very least, to measures being taken which might prevent intra-European solidarity from being subordinated to the imperatives of the solidarity of the English-speaking world.

Mr Schmid's weighty report is rich in information but does not properly address the central issue.
We therefore wish to distance ourselves from it and to reject a procedure which enables this Parliament, on the one hand, to take 'preventive' sanctions against a democratically elected government and, on the other, to refrain from so doing in instances such as this one.

MINORITY OPINION by Maurizio Turco

A. Although the likely existence of an Anglo-American system for the systematic and generalised interception of communications using search engines has been demonstrated, no reference is made to the fact that this technological capacity is certainly being used by Germany and the Netherlands and, probably, by France as well. Accordingly, since the secret services are intercepting communications from abroad, without authorisation and on the grounds of national security, some Member States will be intercepting communications from institutions, citizens or businesses of other Member States.

B. Although more powerful encryption methods should help to protect privacy, their introduction will inevitably lead to the appearance of more powerful lawful means of decryption techniques, given the indissoluble link between the development of cryptographic, code-breaking and technical interception systems.

C. Solutions must therefore be sought in the political field:
- via legal and parliamentary scrutiny of interception activities and monitoring of the police, security and intelligence services;
- by preventing the proliferation of control bodies which operate to different data-protection standards and without any genuine democratic and legal scrutiny,
- by regulating – on the basis of the highest standard and the case-law of the ECHR – protection of the privacy of European citizens against preventive interference by government authorities and eliminating the discrimination existing within the European Union between citizens of various Member States.

Annex I: List of the experts who provided the committee with information

1. Members of national parliaments

Mr Arthur PAECHT, French National Assembly
Mr Armand De DECKER, President of the Belgian Senate
Mrs Anne-Marie LIZIN, Belgian Senate
Mr Hans VAN HEVELE, Secretariat of the Belgian Senate
Mr Guilherme SILVA, Portuguese Parliament
Mr Ludwig STIEGLER, Bundestag (Lower House), Germany
Mr Dieter ANTONI, Austrian Parliament
Mr Desmond O´MALLEY, Irish Parliament

2. Representatives of the secret services

Mr Ernst UHRLAU, Secret Services Coordinator in the Federal Chancellery, Germany
Mr Harald WOLL, Baden-Württemberg Office for the Protection of the Constitution, Germany

3. Telecommunications, network and computer security experts

Mr José Manuel MENDES ESTEVES SERRA VERA, Technical Director, Banco Espirito Santo, Portugal
Mr Clive FEATHER, Head of Software Development, Demon Internet Ltd., United Kingdom
Mr Jacques VINCENT-CARREFOUR, former Head of Department for Network Security, France Telecom
Mr Bruno PELLERO, Expert Consultant in the monitoring of telecommunications, Italy
Mr Erhard MÖLLER, Mr Lutz BERNSTEIN and Mr Bernd SCHINKEN, Higher Institute Aachen, Germany

4. Authors and journalists concentrating on the ECHELON System

Mr Duncan CAMPBELL, United Kingdom
Mr Bo ELKJAER, Denmark
Mr Kenan SEEBERG, Denmark
Mr James BAMFORD, Washington DC
Mr Nicky HAGER, New Zealand

5. Encryption experts

Mr Reinhard WOBST, Unix Software, Germany
Mr Bernd ROELLGEN, Ciphers GmbH, Germany
Mr Peter BAHR, Ciphers GmbH, Germany
Mr Johan KEMPENAERS, KBC Bank, Belgium
Mr Leo VERHOEVEN, KBC Bank, Belgium
Herr Bart PRENEEL, Professor of Cryptology, Catholic University of Louvain, Belgium
Mr Danny de TEMMERMAN, European Commission
Mr Desmond PERKINS, European Commission

6. Experts on industrial espionage and related issues

Mr Sorbas VON COESTER, Director of Salamandre (Consultancy), France
Mr Christian HARBULOT, School for Economic Warfare, France
Mr Thierry LA FRAGETTE, Circé, France
Mr Ralf NEMEYER, Articon-Integralis, Germany

7. Human rights and protection of privacy

Mr Dimitri YERNAULT, Free University, Brussels
Mr Simon DAVIES, Privacy International, United Kingdom
Mr Jérôme THOREL, Privacy International, France
Mr Yaman AKDENIZ, Cyber Rights and Cyber Liberties, Leeds, United Kingdom
Mr David NATAF and Mr Alexandre COSTE, Millet-Sala-Nataf (law practice), Paris
Mr Rüdiger DOSSOW, Council of Europe, Strasbourg

8. Representatives of European Institutions

European Commission
Commissioner Christopher PATTEN (External Relations)
Commissioner António VITORINO (Justice and Home Affairs)
Commissioner Erkki LIIKANEN (Enterprise and the Information Society)
Mr Lodewijk BRIET, Directorate-General for External Relations
Mr Jacques DE BAENST, Head of Protocol and Security
Mrs Françoise DE BAIL, Directorate-General for Trade
Mrs Susan BINNS, Directorate-General for the Internal Market

Council of the European Union
Mr Brian CROWE, Director-General, External Relations
Mr Roland GENSON, Permanent Representative of Luxembourg, with special responsibility for Justice and Home Affairs
Mr Hervé MASUREL, representing the French Council Presidency
Ambassador Gunnar LUND, representing the Swedish Council Presidency

European Central Bank
Mr Christoph BOERSCH, Mr Wolfgang SCHUSTER and Mr Dominique DUBOIS, European Central Bank

9. Interlocutors during missions

Visit by the Chairman and rapporteur to Paris on 18-19 January 2001
Mr Jean-Claude MALLET, Secretary-General of SGDN
Mr Bertrand DUMONT, Air Marshal, Deputy Secretary-General, SGDN
Mrs Claude-France ARNOULD, Director of International and Strategic Affairs, SGDN
Mr Henri SERRES, Director with special responsibility for information systems security, SGDN
Mr Stéphane VERCLYTTE, Legal and European Affairs Adviser, SGDN
Mr Philippe DULUC, Scientific and Technical Affairs Adviser, SGDN
Mr Gérard ARAUD, Director of Strategic Affairs, Foreign Ministry
Mr Olivier MOREAU, Director of Security, Foreign Ministry
Mr Eric PERRAUDAU, Adviser, Defence Ministry
Mr. Jean-Pierre MILLET, lawyer

Visit by the Chairman and rapporteur to London on 24-26 January 2001
Mr Tom KING, Chairman of the Intelligence and Security Committee, House of Commons
Mr Alistair CORBETT, Head of the Secretariat of the ISC, House of Commons
Mr Donald ANDERSON, Chairman of the Foreign Affairs Committee, House of Commons
Mr Bruce GEORGE, Chairman of the Defence Committee, House of Commons
Mr Jack STRAW, Secretary of State for the Home Department
Mr Michael GILLESPIE, Security Service Coordinator
Mr Charles GRANT, Director, Centre for European Reform
Mr Casper BOWDEN, Director of FIPR

Visit by the committee bureau, the coordinators and the rapporteur to Washington DC on 6-12 May 2001
HE Günter BURGHARDT, Head of the Commission Delegation in Washington DC
Mr James WOOLSEY, former Director CIA
Mr Jeffrey RICHELSON, Director, National Security Archive, George Washington University
Mr Marc ROTENBERG, Electronic Information Privacy Centre
Mr Wayne MADSEN, Electronic Information Privacy Centre
Mr David SOBEL, Electronic Information Privacy Centre
Mr Barry STEINHARDT, Associate Director, American Civil Liberties Union
Mr Porter J. GOSS, Chairman of the House Permanent Select Committee on Intelligence
Ms Nancy PELOSI, Vice-Chairman of the House Permanent Select Committee on Intelligence
Mr Robert DAVIS, Deputy Counsel for the Office of Intelligence Policy Review, US Department of Justice.

Annex II: Bibliography

Literature quoted

Advocacy Center, Homepage, http://www.ita.doc.gov/td/advocacy/

Andrew, Christopher, The growth of the Australian Intelligence Community and the Anglo-American Connection, 223-224 in *E. Hayden, H. Peake and S. Halpern* eds, In the Name of Inteligence. Essays in Honor of Walter Pforzheimer (Washington NIBC Press 1995), 95-109

Andrew, Christopher, The making of the Anglo-American SIGINT Alliance, in: *Hayden B. Peake, Halpern, Samuel*. (Eds.): In the Name of Intelligence. Essays in Honor of Walter Pforzheimer, NIBC Press (1995), 95 -109

Andronov, Major *A.*, Zarubezhnoye voyennoye obozreniye, Nr.12, 1993, 37-43

Anonymous, Hacker's guide, Markt &Technik-Verlag (1999)

Bamford, James, Body of Secrets. Anatomy of the Ultra-Secret National Security Agency. From the Cold War through the Dawn of a new Century, Doubleday Books (2001)

Bamford, James, The Puzzle Palace. Inside the National Security Agency, America's most secret intelligence organization, Penguin Books (1983)

Bennett, Gordon, Conflict Studies and Research Center, The Federal Agency of Government Communications and Information, August 2000, http://www.csrc.ac.uk/pdfs/c105.pdf

Berliner Zeitung, Abgehört, 22.1.1996

Bode, Britta, Heinacher, Peter, Sicherheit muß künftig zur Chefsache erklärt werdenn Handelsblatt, 29.8.1996

Brady, Martin, Director of the DSD, Letter dated 16.3.1999 an Ross Coulthart, Sunday Program Channel 9; http://sunday.ninemsn.com/01_cover_stories/transcript_335.asp; http://sunday.ninemsn.com/01_cover_stories/article_335.asp

Bronskill, Jim, Canada a key snooper in huge spy network, Ottawa Citizen, 24.10.2000, http://www.ottawacitizen.com/national/990522/2630510.html

Buchmann, Johannes, Faktorisierung großer Zahlen, Spektrum der Wissenschaft 2, 1999

Bundesministerium für Wirtschaft und Technologie der Bundesrepublik Deutschland, Computerspionage, Dokumentation Nr. 44, Juli 1998

Bundesministerium für Wirtschaft und Technologie der Bundesrepublik Deutschland, Informationen für geheimschutzbetreute Unternehmen (1997)

Bundesverfassungsgericht der Bundesrepublik Deutschland, BVerfG-Urteil, 1 BvR 2226/94 vom 14.7.1999 (zu Art. 10 GG, Gesetz zu Artikel 10 Grundgesetz)

Campbell, Duncan, The state of the art in Communications Intelligence (COMINT) of automated processing for intelligence purposes of intercepted broadband multi-language leased or common carrier systems, and its applicability to COMINT targeting and selection, including speech recognition, Part 2/5, in: STOA (Ed), Development of surveillance technology and risk of abuse of economic information (October 1999), PE 168.184

Campbell, Duncan, Inside Echelon, Heise Online, 24.7.2000, http://www.heise.de/tp/deutsch/special/ech/6928/1.html

Comité permanent de contrôle des services de renseignement, Rapport d'énquête sur la manière dont les services belges de renseignement réagissent face à l'éventualité d'un système americain "echelon" d'interception des communications téléphoniques et fax en Belgique, http://www.droit.fundp.ac.be/textes/echelonfr.pdf

Commission on the Roles and Capabilities of the US Intelligence Community, Preparing for the 21st Century: An Appraisal of U.S. Intelligence, (1996) http://www.gpo.gov/int/report.html

Deutscher Bundestag, Sekretariat des PKGr, Die Parlamentarische Kontrolle der Nachrichtendienste in Deutschland (2000)

Domestic and External Security Secretariat, Department of the Prime Minister and Cabinet (Neuseeland), "Securing our Nation's Safety", Dezember 2000, http://www.dpmc.govt.nz/dess/securingoursafety/index.html

Dodel, Hans, Satellitenkommunikation, Hüthig Verlag (1999),

Elkjaer, Bo & Seeberg, Kenan, Echelon was my baby, Ekstra Bladet, 17.1.1999

Eser, Albin, Überhofer Michael, Huber Barbara (Eds), Korruptionsbekämpfung durch Strafrecht. Ein rechtsvergleichendes Gutachten zu den Bestechungsdelikten im Auftrag des Bayerischen Staatsministeriums der Justiz, edition iuscrim (1997)

Federation of American Scientists (FAS), Homepage, http://www.fas.org/

Fink, Manfred, Lauschziel Wirtschaft - Abhörgefahren und -techniken, Vorbeugung und Abwehr, Richard Boorberg Verlag, Stuttgart (1996)

Förster, Andreas, Maulwürfe in Nadelstreifen, Henschel Verlag (1997)

Frattini, Franco, Il ruolo dei servizi di informazione e sicurezza nel caso 'Echelon'. Relazione del comitato parlamentare per i servizi di informatione e sicurezza e per il segreto di stato. Approvata nella seduta del 29 novembre 2000, Trasmessa alle Presidenze il 19 dicembre 2000.

Freeh, Louis J, Statement for the Record, Hearing on Economic Espionage, House Judiciary Committee, Subcommittee on Crime, Washington DC, 9.5.1996

Freyer, Ulrich, Nachrichten-Übertragungstechnik, Hanser Verlag (2000)

Frost, Mike in a TV interview on NBC's "60 Minutes" on 27.2.2000, http://cryptome.org/echelon-60min.htm

Frost, Mike in an interview on Australian TV‘s Channel 9 on 23.3.1999 http://www.geocities.com/CapitolHill/Senate/8789/sunday1.htm

Frowein, Jochen Abr., Peukert, Wolfgang, Europäische Menschenrechtskonvention[2], N. P. Engel Verlag (1996)

Grant, Charles, Intimate relations. Can Britain play a leading role in European defence - and keep its special links to US intelligence? 4.2000, Centre for European Reform

Guisnel, Jean, L'espionnage n'est plus un secret, The Tocqueville Connection, 10.7.1998

Hager, Nicky, Secret Power. New Zealands´s Role in the International Spy Network, Craig Potton Publishing (1996)

Hager, Nicky, Exposing the global surveillance system, http://www.ncoic.com/echelon1.htm

Hoffmann, Wolfgang, Arbeitsgemeinschaft für Sicherheit der Wirtschaft e.V. (ASW), Aktuelle Anmerkungen zur Sicherheitslage der deutschen Wirtschaft, April 2001

Hummelt, Roman, Wirtschaftsspionage auf dem Datenhighway, Strategische Risiken und Spionageabwehr, Hanser Verlag (1997)

Intelligence and Security Committee (UK), Annual Report 1999-2000

Jacobs, Francis G, White, Robin C.A., The European Convention on Human Rights[2], Clarendon Press (1996)

Jauvert, Vincent, Espionnage - comment la France écoute le monde, Le Nouvel Observateur, 5.4.2001, Nr. 1900, S. 14 ff.

Kreye, Andrian, Aktenkrieger, Süddeutsche Zeitung, 29.3.2001

Kuppinger, Martin, Internet- und Intranetsicherheit, Microsoft Press Deutschland (1998), 60

Kurtz, George, McClure, Stuart, Scambray, Joel, Hacking exposed, Osborne/McGraw-Hill (2000)

Kyas, Othmar, Sicherheit im Internet, International Thomson Publishing (1998), 23

Landesamt für Verfassungsschutz Baden Württemberg, Wirtschaftsspionage, Die gewerbliche Wirtschaft im Visier fremder Nachrichtendienste, 10/1998

Legal Standards for the Intelligence Community in Conducting Electronic Surveillance, Report to the US Congress in late February 2000, http://www.fas.org/irp/nsa/standards.html

Leiberich, Otto, Vom diplomatischen Code zur Falltürfunktion - Hundert Jahre Kryptographie in Deutschland, Spektrum der Wissenschaft, Juni 1999

Lyle Robert, Radio Liberty/Radio Free Europe, 10 February 1999

National Security Councils (NSC), Homepage, http://www.whitehouse.gov/nsc

Madsen, Wayne in a TV interview on NBC's "60 Minutes" vom 27.2.2000, http://cryptome.org/echelon-60min.htm

Paecht, Arthur, Rapport d'information déposé en application de l'article 145 du règlement par la commission de la défense nationale et des forces armées, sur les systèmes de surveillance et d'interception électroniques pouvant mettre en cause la sécurité nationale, N° 2623 Assemblée nationale, enregisté à la Présidence de l'Assemblée nationale le 11 octobre 2000.

Paecht, Arthur, Rapport fait au nom de la Commission de la défense nationale et des forces armées sur la proposition de loi (N° 1497) de M. Paul Quilès et plusieurs de ses collègues tendant à la création d'une délégation parlementaire pour les affaires de renseignement, enregistré à la Présidence de l'Assemblée nationale le 23 novembre 1999

Porter, Michael E., Competitive Strategy, Simon & Schuster (1998)

Richelson, Jeffrey T., Desperately seeking Signals, The Bulletin of the Atomic Scientists Vol. 56, No. 2/2000, pp. 47-51, http://www.bullatomsci.org/issues/2000/ma00/ma00richelson.html

Richelson, Jeffrey T., The U.S. Intelligence Community[4], Westview Press, 1999

Richelson, Jeffrey T., The National Security Agency Declassified, National Security Archive Electronic Briefing Book no. 24, George Washington University http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB23/index.html

Richelson, Jeffrey T., Ball, Desmond, The Ties That Bind, Boston Unwin Hyman (1985)

Richter, Nicolas, Klettern für die Konkurrenz, Süddeutsche Zeitung, 13.9.2000

Rötzer, Florian, Die NSA geht wegen Echelon an die Öffentlichkeit, Heise Online, 26.02.2000, http://www.heise.de/bin/tp/issue/download.cgi?artikelnr=6633&rub_ordner=special

Schmidt-Eenboom, Erich, Streng Geheim, Museumsstiftung Post und Telekommunikation Heidelberg, (1999)

Schütze, Arno, Wirtschaftsspionage: Was macht eigentlich die Konkurrenz? P.M. Magazin, Die Moderne Welt des Wissens (1998)

Shane Scott, Bowman Tom, America's Fortress of Spies, Baltimore Sun, 3.12.1995

Simon Singh, Geheime Botschaften, Carl Hanser Verlag (1999)

Smith, Bradley F., The Ultra-Magic Deals and the Most Secret Special Relationship 1940-1946, Presidio (1993)

Sorti, Francesco, Dossier esclusivo. Caso Echelon. Parla Luigi Ramponi. Anche I politici sapevano, Il Mondo, 17.4.1998

State Department Foreign Press Center Briefing, Subject: Intelligence Gathering and Democracies: The Issue of Economic and Industrial Espionage, Washington DC, 7.3.2000

Süddeutsche Zeitung, Haftstrafe wegen Spionage für Russland, 30.5.2000

TPCC, Broschüre über das Advocacy Center, Oktober 1996

Thaller, Georg Erwin, Satelliten im Erdorbit. Nachrichten, Fernsehen und Telefonate aus dem Weltall, Franzis Verlag, München (1999)

White House Archives http://govinfo.library.unt.edu/npr/library/direct/orders/tradepromotion.html

Wessely, Wolfgang, Das Fernmeldgeheimnis - ein unbekannts Grundrecht?, ÖJZ 1999, 491 ff

Wirtschaftswoche "Antennen gedreht", Nr. 46/9, November 1999

Wirtschaftswoche "Nicht gerade zimperlich", Nr. 43/16, Oktober 1992

Wobst, Reinhard, Abenteuer Kryptologie, Adison-Wesley (1998)

Woolsey, James, Why America Spies on its Allies, The Wall Street Journal Europe, 22.3.2000

Woolsey, *James,* Remarks at the Foreign Press Center, Transscript, 7.3.2000, http://cryptome.org/echelon-cia.htm

Wright, Steve, An appraisal of technologies for political control, STOA interim study (1998) PE 166.499/INT.ST.

Yernault, Dimitri, "Echelon" et l'Europe. La protection de la vie privée face à l'espionnage des communications, Journal des tribunaux, Droit Européen 2000, p. 187 ff.

FOR FURTHER READING

Air Intelligence Agency (AIA), Homepage, http://www.aia.af.mil

America´s Military Community, Homepage, http://www.military.com

Barr, Bob, Barr moves to expose "Project ECHELON", 9.11.1999, http://www.house.gov/barr/p_110999.html

Bundesnachrichtendienst, Die Nachrichtendienste der Bundesrepublik Deutschland, 2000, http://www.bundesnachrichtendienst.de/diensteb.htm

Bundesamt für Verfassungsschutz, Spionage gefährdet die Sicherheit und die Interessen unseres Landes, 2001, http://www.verfassungsschutz.de/arbeitsfelder/spion/page.html

Campbell, Duncan, Somebody´s listening, They´ve got it taped, 12.8.1988, New Statesman, http://jya.com/echelon-dc.htm

Central Intelligence Agency (CIA), Homepage http://www.odci.gov/index.html

Commander Submarine Force, U.S. Atlantic Fleet - Surveillance and Intelligence, http://www.sublant.navy.mil/roles.htm#survintel

Collingwood, John, Carnivore Diagnostic Tool, 16.8.2000, FBI-Press-Room http://www.fbi.gov/

Ecole de Guerre Economique, Homepage, http://www.ege.eslsca.fr/

Federal Bureau of Investigation (FBI), Homepage, http://www.fbi.gov

Frankfurter Allgemeine Zeitung, Niederländische Wirtschaftsspionage, 19.4.2000

Frankfurter Allgemeine Zeitung, Wirtschaftsspionage, 3.2.2001

Freeh, J. Louis, International espionage, 28.2.1996, Address before the Senate, http://www.fbi.gov

General Dynamics, Seawolf Class, http://www.gdeb.com/programs/seawolf/

Göbel, Jürgen, Kommunikationstechnik, Grundlagen und Anwendungen, Hüthig (1999)

Goss, J. Porter, Additional views of chairman Porter J. Goss, 2000, http://www.aclu.org/echelonwatch/goss.htm

Gralla, Preston, So funktioniert das Internet: ein virtueller Streifzug durch das Internet, Markt und Technik (1999)

Hager, Nicky, Wie ich Echelon erforscht habe, 11.04.2000, http://www.heise.de/tp/deutsch/special/ech/6728/1.html

Hayden, Michael, Statement for the record of House Permanent Select Committee on Intelligence, 12.04.2000 http://www.nsa.gov/releases/DIR_HPSCI_12APR.HTML

Innenministerium Brandenburg, Abwehr von Wirtschaftsspionage, 1999

Kerr, M. Donald, Congressional Statement on Carnivore Diagnostic Tool, 6.9.2000, http://www.fbi.gov

Kerr, M. Donald, Congressional Statement on Internet and Data-Interception Capabilities Developed by the FBI, 24.7.2000, http://www.fbi.gov

Mass, Christian, Satelliten Signale anzapfen und auswerten, Satellitenspionage für Einsteiger, Franzis Verlag, Funkschau Telekom, Poing 1998

Mathiesen, Thomas, On Globalisation of Control: Towards an Integrated Surveillance System in Europe, Statewatch Publication, 11.1999

Matschke, Klaus Dieter, Geheimdienste im Auftrag des Wettbewerbs, 5.9.1998, Seku Media Verlag Ingelheim

National Security Agency (NSA), Homepage, http://www.nsa.gov/

Preneel, Bart, Relative Security of Cryptographic, 18.11.1998, Presentation to Conference on Problems of Global Security

Schönleber, Claus, Verschlüsselungsverfahren für PC-Daten, Franzis Verlag, Poing 1995

Secretary of State for the Home Department, Interception of communications in the UK, June 1999

Sénat et Chambre des représentants de Belgique, 14.2.2000, Rapport d´activités 1999 du Comité permanent de contrôle des services de renseignements et de sécurité

Tenet, George, Statement by Director of Central Intelligence before the House Permanent Select Committee on Intelligence, 12.4.2000, http://sun00781.dn.net/irp/congress/2000_hr/tenet.html

The United States Navy, Homepage, http://www.navy.mil

The US Army Intelligence and Security Command (INSCOM), Homepage http://www.vulcan.belvoir.army.mil

The White House, Defending America's Cyberspace, National Plan for Information Systems Protection, Version 1.0, 2000, The White House 2000

Ulfkotte, Udo, Marktplatz der Diebe, Wie die Wirtschaftsspionage deutsche Unternehmen ausplündert und ruiniert. Bertelsmann Verlag, München (1999)

V. Bülow, Andreas, Im Namen des Staates. CIA, BND und die kriminellen Machenschaften der Geheimdienste. Piper Verlag, München (1998)

Verfassungsschutz Brandenburg, Abwehr von Wirtschaftsspionage - eine Aufgabe des Verfassungsschutzes, 1999, http://www.brandenburg.de/land/mi/vschutz/wispion.htm

Wall, Stephen, Permanent Representative of the United Kingdom to the European Union, Letter to Commissioner Liikanen concerning GCHQ, 21.3.2000

Wojahn, Jörg, Die globalen High-Tech-Schnüffler, 1.9.2000, Der Standard

Annex III: Definitions and explanations concerning the interception of communications for the purpose of criminal prosecution

1. Preliminary remarks

During the discussion in committee about the reliability, impact and dangers of the interception systems used world-wide by various intelligence services, reference was repeatedly made to measures and activities within the EU which, while involving the interception of communications, fell under the heading of judicial cooperation in criminal matters.
In the first part of this report, your rapporteur has, therefore, made no reference to those measures, since the issue of the legitimacy of intercepting communications for the purposes of criminal prosecution must not be confused with the legitimacy of intercepting communications for the purposes of intelligence gathering. Although interference in the private sphere, justified on security grounds (in the broadest sense of the term), is involved in both instances, the working methods and objectives are so different from each other that rules which might appear reasonable and balanced in one field would not necessarily be so for the other. The pertinence and proportionality of criminal prosecution measures should, therefore, not be discussed against the background of a political appraisal of measures relating to intelligence gathering.
At this juncture, in order to eliminate any uncertainties, reference will be made to particular issues raised, and definitions will be given of specific terms. Initially, a distinction will be drawn in Section 2 below between interception of communications for the purpose of criminal prosecution and interception for the purpose of intelligence gathering. Subsequently, in Section 3, reference will be made, with due account being taken of its powers and responsibilities, to EU legal acts involving interception of communications for the purpose of criminal prosecution. Finally, in Section 4, an explanation will be given of other terms used repeatedly in the committee's discussions in the context of international activities in the field of interception of communications.

2. Distinction between the interception of communications for the purpose of criminal prosecution and for the purpose of intelligence gathering

Interception of communications by foreign intelligence services (for example, by what is known as the ECHELON system) does not seek to monitor individuals in their home country but to carry out a general interception of traffic in a foreign country or countries in order, principally, to secure information which is relevant to national security. It is carried out in secret and, in the long term, does not aim to enter the public domain. Using the argument that secrecy alone can guarantee security and that they do not involve their own nationals, the secret services are frequently allowed to operate in a grey area as far as the law is concerned, where the rules are opaque and scrutiny inadequate.

On the other hand, where adequate suspicion exists, interception of communications for the purpose of criminal prosecution aims at preventing an offence from being committed or at punishing offences already committed. The interception measures are determined by the authorities in their home country. Should interception measures be required in a foreign

country, they are taken by the authorities in that country, on the basis of letters rogatory. Since the abolition of the police state, because the measures involve nationals, very specific rules and efficient control mechanisms have been established which seek to achieve a balance of interests. Interception measures may, therefore, be determined solely with regard to a specific case and where there is adequate suspicion that an offence may be about to be, or may have been, committed. In many Member States, court authorisation is required. Although the interception is carried out in secret, it aims solely at securing evidence to be used in open court. Accordingly, it is in the authorities' own interests to ensure that such evidence is acquired lawfully.

3. Activities in the EU in the field of interception of communications for the purpose of criminal prosecution

3.1. General remarks

The insertion in the Treaty on European Union of a Title relating to the common foreign and security policy created an opportunity for intelligence services to cooperate at European level, an opportunity which, however, has not to date been seized.
Where rules have been laid down and work has been carried out in the field of interception of communications at EU level, they have involved solely the criminal prosecution side, i.e. cooperation on matters relating to Justice and Home Affairs.

3.2. Restriction of EU powers and responsibilities to technical arrangements

As things stand, rules governing the admissibility of interception measures fall exclusively within the remit of the Member States. In accordance with the principle of limited powers, the EU may act only where powers and responsibilities are entrusted to it on the basis of the treaties. However, no provision is made for any such powers and responsibilities in Title VI of the EU Treaty entitled 'Provisions on police and judicial cooperation in criminal matters'. In the field of police cooperation, Article 30(1) of the TEU provides for common action solely with regard to operational aspects, i.e. those which concern the ways and means of carrying out police work. In the field of judicial cooperation in criminal matters, although Article 31(c) provides in general terms, within the ambit of common action, for 'ensuring compatibility in rules applicable in the Member States', that is authorised only in so far 'as may be necessary to improve [such] cooperation'. In other words, it is geared to cooperation-specific rules. Furthermore, the 'approximation of rules on criminal matters' in the Member States' pursuant to the final indent of Article 29 restricts itself to the establishment of minimum rules relating to the constituent elements of criminal acts (Article 31(e)). To sum up, we may say that a decision on the issue of the conditions under which interception of communications is admissible remains a matter exclusively for national law. Your rapporteur is not aware of any efforts being made by any Member State to make changes to this purely national competence.

Cooperation between the Member States on the basis of the treaties may therefore come into play only when the issue is debated of the implementation of interception measures taken in accordance with national law, i.e. at a lower level. In instances where, on the basis of national law, interception of telecommunications is authorised, the Member State involved should be

able to call on the other Member States for technical assistance. Whether the technical simplification sought, which would without doubt improve the efficiency of transfrontier interception of communications for the purpose of criminal prosecution, particularly in the field of organised crime, is held to be good or bad depends largely on the extent of confidence felt in the constitutional state involved. However, it should be emphasised once again that – even if transfrontier interception of communications is technically simplified by the introduction of technical uniformity, and even if abuse in individual cases cannot be prevented – the conditions for the admissibility of interception cannot be affected since they are governed exclusively by national law.

3.3. Activities and legal acts in the field of interception of telecommunications

Only two legal acts have been adopted in the field of interception of telecommunications: the Council Resolution of 17 January 1995 on the lawful interception of telecommunications, the substance of which should be extended to cover third countries by means of a corresponding Memorandum of Understanding and in respect of which, furthermore, a proposal for an update was planned (both were drawn up as ENFOPOL documents), and the agreement on judicial assistance in criminal matters.

Council Resolution of 17 January 1995 on the lawful interception of telecommunications[262]

The Council Resolution of 17 January 1995 on the lawful interception of telecommunications seems to go back to the cooperation between experts in the International Law Enforcement Telecommunications Seminar (ILETS) (see Section 4 below) and largely to comply with the IUR (international user requirements) drawn up thereat.
The aim of the resolution is to seek to ensure that the requisite technical conditions are created in all the Member States and that the authorities, in accordance with national authorisation procedures, may actually obtain access to data, thus being able to exercise the powers granted to them by national law at the technical level.
To that end, an annex includes a very detailed list of Member States' 'Requirements'. The Council 'notes' that the Requirements 'constitute an important summary of the needs of the competent authorities for the technical implementation of legally authorised interception in modern telecommunications systems.' Such requirements include, for example, the provision of call-associated data in real time and the ability of network operators to transmit the intercepted communications to the law enforcement monitoring facility. In the resolution, the Council considers that the Requirements should be 'taken into account in the definition and implementation of measures …' and calls on the Member States and the Ministers responsible 'to cooperate … with the aim of implementing the Requirements in relation to network operators and service providers.'
At this juncture, it should be emphasised that the form of legal act selected – a resolution – is not binding in nature and that it therefore creates no rights and obligations for the Member States. The controversy which surrounded the resolution and the documents appertaining thereto resulted not so much from its substance but rather from the circumstances in which it was drawn up, in particular from the lack of transparency.

[262] OJ C 329, 4.11.1996.

Memorandum of Understanding

In a subsequent Memorandum of Understanding[263], third countries were invited to transpose into their national law the technical Requirements set out in the resolution of 17 January 1995. In addition, the aim was for technical innovations and the resultant new Requirements to be notified to both the FBI and the Council Secretariat. That was done because intelligence technology is frequently manufactured by multinational undertakings. Accordingly, cooperation was essential with the interception authorities in third countries where production plants were located.
The Memorandum of Understanding was signed on 23 November 1995 by the Member States of the EU and Norway, but not by any other third countries. The USA, Australia and Canada simply informed the Council in writing that they would initiate the process for the transposition of the provisions into national law[264].
Unfortunately, that text has still not been published, a fact which has given rise to extensive speculation in the press.

Draft Council resolution on the lawful interception of telecommunications in relation to new technologies

As your rapporteur pointed out in his report dated 23 April 1999[265], the draft Council resolution on the lawful interception of telecommunications in relation to new technologies is an update of the 1995 resolution. The new resolution is designed to make it clear that the 1995 Council resolution, which will be supplemented by a few new Requirements, also applies to new communications technologies, such as satellite and Internet communications, and that the previously used technical terms are to be interpreted, mutatis mutandis, with regard to the new technologies (e.g. telephone number recognition in the Internet). The European Parliament approved the draft[266], but the Council has temporarily shelved the project.

Convention on Mutual Assistance in Criminal Matters[267]

The second legal act is the Convention on Mutual Assistance in Criminal Matters. Articles 17 et seq. thereof lay down the conditions in which mutual assistance in criminal matters is possible with regard to interception of telecommunications. Without going into the rules in detail, your rapporteur would point out that the Convention in no way curtails the rights of the

[263] No 10.037/95 ENFOPOL 112 (unpublished).
For the substance, see the written answer given by the Austrian Interior Minister, Karl Schlögel, dated 16 December 1998 to the Written Question tabled by Alexander Van der Bellen, MP; 4739/AB XX. GP.
[264] To quote the Austrian Interior Minister, Karl Schlögel, (see previous footnote). The President-in-Office of the Council, Michiel Patijn, said, somewhat opaquely, in his answer to Oral Question H-0330/97 by Jonas Sjöstadt at Question Time on 14 May 1997 that 'these Requirements' (he was referring to the Requirements set out in the Council Resolution of 17 January 1995) had also been signed by the United States, Canada, Australia and Norway.
[265] A4-0243/99.
[266] Legislative resolution embodying the opinion of the European Parliament adopted on 7 May 1999 (OJ C 279, 1.10.1999, p. 498).
[267] Council Act of 29 May 2000 establishing in accordance with Article 34 of the Treaty on European Union the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union, OJ C 197, 12.7.2000, p. 1, Articles 17 et seq.

person or persons whose communications are intercepted, since the Member State in which the person or persons whose communications are intercepted is located may at all times refuse assistance if such assistance is not permitted under its own national law.

4. Definitions and explanations concerning further international activities in the field of interception of telecommunications

It is not only the various EU legal acts but also the disparate working parties set up in the field of security policy which have caused confusion. Some of the terms are therefore clarified below.

ILETS (International Law Enforcement Telecommunications Seminar)

ILET Seminars were originally an FBI initiative. In 1993, the FBI invited criminal prosecution authorities and intelligence services from friendly countries to attend a seminar on telecommunications interception being held in Quanitco. Most of the current Member States of the EU, as well as Australia and Canada, attended the seminar[268]. Since then, regular meetings have been held in order to discuss requirements for efficient international communications interception.
At a meeting held in Bonn in 1994, the members of ILETS approved a document setting out policy guidelines, an annex to which included a list of international user requirements (IUR 1.0 or IUR 95). That list included the Requirements to be imposed on the various telecommunications operators in order to simplify the interception system. The IUR 1.0 served – albeit unofficially – as the basis for the Council Resolution of 17 January 1995 on the lawful interception of telecommunications. Subsequently, further meetings of experts were held to discuss IUR and their possible transposition and adjustment to cope with new telecommunications technologies.

TREVI Group

Meeting as the Trevi Group before the entry into force of the Treaty of Maastricht (which introduced provisions to govern cooperation in the fields of justice and home affairs in the Treaty on European Union), the Justice and Home Affairs Ministers discussed internal security issues. The Trevi Group is now defunct, since the topics involved are now dealt with in specific Council working parties.
With respect to the field at issue here, specific reference should be made to two such working parties, the Working Party on Mutual Assistance in Criminal Matters - which, as part of the activities for cooperation in justice and home affairs, dealt with the Convention on Mutual Assistance in Criminal Matters - and the Working Party on Police Cooperation, which was concerned with issues connected with the lawful interception of telecommunications traffic, including the monitoring of new communications systems (mobile telephones, Internet, e-mail). The latter was also involved in the approximation of the standards of the Requirements of the authorities competent to order interception of telecommunications imposed on network operators and service suppliers.

[268] For the substance of that seminar, see the written answer given by the Austrian Interior Minister, Karl Schlögel, to the Question tabled by Mr Van der Bellen, MP. 4014/AB XX.GP. http://www.parlinkom.gv.at/pd/pm/XX/AB/texte/AB04014_.html.

ENFOPOL

Despite the belief held by a number of writers, ENFOPOL is not a working party or an organisation, it is an abbreviation used for the designation of working papers in criminal prosecution and police matters drawn up, for example, by the Working Party on Police Cooperation[269]. The various documents are not given an ENFOPOL title, they are simply classified under that reference.

[269] See the oral answer given by Austrian Interior Minister, Karl Schlögel, to the Question tabled by Mr Van der Bellen, MP, 4739/AB XX.GP http://www.parlinkom.gv.at/pd/pm/XX/AB/texte/040/AB04014_.shtml and Campbell, Duncan, ILETS, the secret hand behind ENFOPOL 98, http//heise.de/deutsch/special/enfo/6396/1.html.

ANNEX IV

SUMMARY

OF THE

INTELLIGENCE SERVICES AND PARLIAMENTARY CONTROL BODIES

OF THE

MEMBER STATES AND OF THE UKUSA STATES

Country	Intelligence service	Legal basis	Duties	SIGINT capacity	Control authority	Le
AUSTRIA	***Heeresnachrichtenamt (HnA)*** ***Abwehramt (AbwA)*** military intelligence service reports to the Minister of Defence	*§ 20 Abs 3 Militärbefugnisgesetz (MBG) BGBl I 86/2000'*	military intelligence; counter-intelligence to combat threats to national security from abroad		parliamentary subcommittee: *Ständiger Unter-ausschuss des Landesverteidigungs-ausschusses zur Überprüfung von nachrichten-dienstlichen Maß-nahmen zur Siche-rung der militärischen Landesverteidigung (14 members; each party in Parliament must be represented)* *1 legal protection representative*	*A* *B* *g* *§* *G* *1*

Country	Intelligence service	Legal basis	Duties	SIGINT capacity	Control authority	Le
AUSTRIA	**Sondereinheit für Observation (SEO)** civil intelligence service reports to the Minister of the Interior	*§§ 6, 14, 15 Sicherheitspolizei-gesetz (SPG, BGBl 566/1991 idgF);* *Sondereinheiten-Verordnung* (BGBl II 207/1998)	preserving public safety; internal counter-intelligence; protecting principles guaranteed by the Constitution; counteracting extremist movements, terrorism and organised crime		parliamentary subcommittee: *Ständiger Unter-ausschuss des Ausschusses für innere Angelegen-heiten zur Über-prüfung von Maß-nahmen zum Schutz der verfassungs-mäßigen Einrichtungen und ihrer Handlungs-fähigkeit* *(14 members; each party in Parliament must be represented)* *1 legal protection representative*	

Country	Intelligence service	Legal basis	Duties	SIGINT capacity	Control authority	Le
BELGIUM	**Service Général du Renseignement et de la Sécurité des Forces armées(SGR)** **military intelligence and security service** reports to the Minister of Defence	*Loi du 30 novembre 1998 organique des services de renseignement et de sécurité*	obtaining information and data in the military, political, economic and technological/scientific field, responsible for the security of military installations and personnel		*Comité permanent de contrôle des services de renseignements et de sécurité (Comité permanent R),* three members appointed by the Senate; they may not hold electoral office or carry out any other activity that might jeopardise their independence *Service d'enquêtes des services de renseignements* attached to the Comité permanent R, members appointed by the Comité R	*Lo (V co de re*
BELGIUM	**Sûreté de l'Etat (VS)** **civil intelligence and security service** reports to the Minister of Justice	*Loi du 30 novembre 1998 organique des services de renseignement et de sécurité*	responsible for internal and external security, counter-intelligence, observation of political extremism			

Country	Intelligence service	Legal basis	Duties	SIGINT capacity	Control authority
DENMARK	Forsvarets Efterretningstjeneste (FE(T)) **'Military Secret Service'** reports to the Minister of Defence	*Lov om forsvarets formål, opgaver og organisation m.v.* *Lov 909 af 8/12/1993* ['framework-law', in which FE(T) is not mentioned] [a new law on FET & PET will be adopted in the near future]	collecting and analysing secret information relevant to defence on the CIS, Central and Eastern Europe in the military, political, economic and technological/scientific fields, SIGINT; decryption staff & budget: classified information	yes	2 control committees: *Kontroludvalget vedrørende Politiets og Forsvarets efterretningstjenester (Wamberg-udvalget) (consisting of civil servants and lawyers)* appointed by the Minister of Justice *Udvalget vedrørende efterretningstjenesterne* parliamentary committee (consisting of 5 Members of the Danish Parliament)

Country	Intelligence service	Legal basis	Duties	SIGINT capacity	Control authority
DENMARK	Politiets Efterretningstjeneste (PET) **'Police Secret Service'** reports to the Minister of Justice	no specific legislation [a new law on FET & PET will be adopted in the near future]	counter-intelligence, prevention of and action against activities which might endanger Denmark's security: espionage, terrorism, etc.; security of the Government and of the Royal Family staff: about 370 (1998) budget: classified information.		

Country	Intelligence service	Legal basis	Duties	SIGINT capacity	Control authority	Le
FINLAND	**Pääesikunnan tiedusteluosasto 'Military Intelligence Division of the Finnish Defence Staff'** reports to the Minister of Defence	*Laki puolustusvoimista* N:o 402/1974 2§ 'Defence Forces Act' (Intelligence Division not mentioned)	surveillance of the country's land and sea areas and airspace in cooperation with other supervisory authorities, ensuring territorial integrity of the country	yes	no specific control body Ministry of Defence submits an annual report on interception to the Parliamentary Ombudsman	*P* *§3* 'P *La* *m* *40* 'C Ac [c Pa O re re M

Country	Intelligence service	Legal basis	Duties	SIGINT capacity	Control authority	Le
FINLAND	**Suojelupoliisi (SUPO) 'Finnish Security Police'** reports to the Minister of the Interior	*Laki poliisin hallinnosta N:o 110/1992, 1§, 10§ 1. ja 2. momentti* *Asetus poliisin hallinnosta N:o 158/1996 8§* *Laki poliisin henkilörekistereistä N:o 509/1995 23§, 9§* 'Act and Decree on Police Administration', 'Police Personal Data' Act	counter-intelligence; averting activities which might endanger Finland's internal security and international relations, action against terrorism, preventive work for security		no specific control body; the police has to report all cases of interception to the Minister of the Interior, who submits an annual report to the Parliamentary Ombudsman	
FINLAND	**Tullin tiedusteluyksikkö 'Intelligence Section of the Finnish Customs'** reports to the Ministry of Finance	*Tullilaki N:o 1466/1994* 'Customs Act'	collecting and analysing data to prevent and uncover customs offences, and supplying such data to the relevant authorities for further action		no specific control body the customs have to report all cases of interception to the National Customs Board and to the Minister of the Interior, who submits an annual report to the Parliamentary Ombudsman	

Country	Intelligence service	Legal basis	Duties	SIGINT capacity	Control authority	Le
FRANCE	**Direction générale de la sécurité extérieure (DGSE)** reports to the Ministry of Defence	*Décret n°82-306 du 2 avril 1982*	collecting intelligence data of political, economic and technological/scientific relevance, collecting and analysing intelligence of interest to the security of France, counter-espionage (outside national territory) 4100 Staff Budget: FF 1.7 billion	yes	no special parliamentary control body at the moment (under discussion; the Defence Committee of the National Assembly has twice proposed that a surveillance-type committee should be established; Nos 1951 and 2270) Commission nationale de contrôle des interceptions de sécurité' (exclusively scrutiny of interception of communications by means of wire-tapping) Members of this body include 1 MP and 1 Senator	

Country	Intelligence service	Legal basis	Duties	SIGINT capacity	Control authority	Le
FRANCE	**Direction du renseignement militaire (DRM)** reports to the Ministry of Defence	*Décret n°92-523 du 16 juin 1992*	provides military intelligence necessary for the armed services 1700 staff, Budget FF 90 million, internal military security, supporting the army;			
FRANCE	**Direction de la surveillance du territoire (DST)** Civilian intelligence service reports to the Minister of the Interior	*Décret n°82-1100 du 22 décembre 1982*	Counter-espionage on French territory 1500 staff; protecting public safety, internal counter-intelligence			

Country	Intelligence service	Legal basis	Duties	SIGINT capacity	Control authority	Le
GERMANY	**Bundesnachrichten-dienst (BND)** reports to the Federal Chancellor	*Gesetz über den Bundesnachrichten-dienst (BNDG),* BGBl 1990 I 2954 idgF	collecting and analysing intelligence on foreign activities of relevance to security and foreign policy	yes	*Parlamentarisches Kontrollgremium (PKGR*) parliamentary control body for all 3 secret services consists of 9 MPs (Members of the Bundestag)	*G Ko di de (P 19 id*
GERMANY	**Bundesamt für Verfassungsschutz (BfV)** reports to the Minister of the Interior	*Gesetz über die Zusammenarbeit des Bundes und der Länder in Angele-genheiten des Ver-fassungsschutzes und über das Bundsamt für den Verfassungs-schutz* (BVerfSchG, BGBl 1090 I 2954)	collecting and analysing intelligence on activities endangering security and activities of hostile intelligence services within Germany		*G 10-Kommission* not bound to take instructions; may, but need not, include MPs; 4 Members appointed by the PKGR	*§ G G (G A 94 (L Pe Te Se*
GERMANY	**Militärischer Abschirmdient (MAD)** reports to the Minister of Defence	*Gesetz über den militärischen Ab-schirmdienst (MADG*) BGBl 1990 I 2954 idgF	safeguarding the army's effectiveness protecting the security of military installations and military personnel			

Country	Intelligence service	Legal basis	Duties	SIGINT capacity	Control authority	Le
GREECE	Ethniki Ypiresia Pliroforion (EYP) 'National Intelligence Service' reports to the KYSEA (National Security Council: Prime Minister + Ministers of Foreign Affairs and Defence)	Law 1645/86 on the National Intelligence Service *(Ethniki Ypiresia Pliroforion)*	* collecting and analysing information pertaining to the country's national security (information on organised crime, terrorism, military, economic and political information); forwarding of such information to the competent authorities * counter-intelligence; observation of activities of foreign intelligence services directed against the country.		Special parliamentary committee for the protection of communications and privacy. No specific control rights. Membership: 1 Vice-President of Parliament, 1 Member of each political group, 1 communications specialist	La *Ap* (S co
					Institution for the Protection of Personal Data	La *Pr* *ep* *de* *pr* (P Pe

Country	Intelligence service	Legal basis	Duties	SIGINT capacity	Control authority	Le
IRELAND	**Garda Síochána** (national police service) deals with national security issues The police service reports to the Minister of Justice	Authority to intercept based on *Interception of Postal Packets and Telecommunications Messages (Regulation) Act 1993*	Interception authorised in the interests of the security of the State		*Joint Committee on Justice, Equality and Women's Rights* has responsibility for the general area of civil rights	
IRELAND	Intelligence Staff		national security interests of Ireland (mainly the IRA), security of national armed forces, technological developments of foreign armed forces		No special control authority	

Country	Intelligence service	Legal basis	Duties	SIGINT capacity	Control authority	Le
ITALY	**Servizio per le informazioni e la sicurezza militare (SISMI)** **Servicio informazione operative Segrete (SIOS)** reports to the Minister of Defence who also appoints the Director of the Service and senior civil servants	*L. 24 ottobre 1977, n. 801, art. 4 Istituzione e ordinamento dei servizi per le informazioni e la sicurezza e disciplina del segreto di Stato*	Military defence intelligence and security duties to protect the independence and integrity of the State, counter-espionage, collecting foreign intelligence on political, military, economic and technological/scientific subjects	yes	Parliamentary Committee (4 MPs + 4 Senators) The Government submits a six-monthly report to Parliament on information and security policy	L. 80 *Is* *or* *se* *in* *si* *de*
ITALY	**Servizio per le informazioni e la sicurezza democratica (SISDE)** **Direzione investigazioni anti-mafia (DIA)** reports to the Minister of the Interior who also appoints the Director of the Service and senior civil servants	*L. 24 ottobre 1977, n. 801, art. 6 Istituzione e ordinamento dei servizi per le informazioni e la sicurezza e disciplina del segreto di Stato*	intelligence and security duties for the defence of the democratic State and its institutions intelligence on activities endangering internal security; counter-espionage to combat terrorism and organised crime			

Country	Intelligence service	Legal basis	Duties	SIGINT capacity	Control authority	Le
LUXEM-BOURG	**Service de renseignement** national intelligence and security service reports to the Minister of State (= Prime Minister)	*Loi concernant la protection des secrets intéressant la sécurité extérieure de l'État du 30 juillet 1960*	protecting secrets under Article 120(vii) of the Criminal Code* and obtaining information necessary to safeguard the external security of the Grand Duchy and States with which it has concluded a regional joint defence agreement * 'offences against the GD of Luxembourg'		no parliamentary scrutiny (surveillance of any kind of communications to seek out offences against State security requires the assent of a committee comprising the chairman of the Supreme Court, the chairman of the Legal Affairs Committee of the Council of State and the chairman of the Chamber of Auditors)	*(L 19 in d' de 88*

Country	Intelligence service	Legal basis	Duties	SIGINT capacity	Control authority	Le
NETHER-LANDS	**Militaire Inlichtingendienst (MID** or, more recently, MIVD) reports to the Ministry of Defence	*Wet op de inlichtingen- en veiligheidsdiensten* Law 635/87 of 3 December 1987, most recently amended by Law 194/1999 of 19 April 1999. [New bill under discussion]	military intelligence; intelligence-gathering on foreign armed forces	yes	*Tweede-Kamercommissie voor de Inlichtingen- en veiligheidsdiensten* 'Second Chamber Committee for Information and Security Services' parliamentary committee (4 members: the chairmen of the 4 major political parties)	*17 or Ka G* R N C '(In Se
NETHER-LANDS	**Binnenlandse Veiligheidsdienst** (**BVD** or, more recently, AIVD) reports to the Ministry of the Interior		Internal security service, counteracting right- and left-wing extremism, counter-intelligence			

Country	Intelligence service	Legal basis	Duties	SIGINT capacity	Control authority	Le
PORTUGAL	**Serviçio de Informações Estratégicas de Defesa e Militares (SIEDM)** reports to the Minister of Defence	Law 30/84 of 5 September 1984, amended by Law 4/95 of 21 February 1995, Law 15/96 of 30 April 1996 and Law 75-A/97 of 22 July 1997	foreign intelligence service; strategic intelligence service for political, military and economic affairs		*Conselho de Fiscalização dos Serviços de Informações (CFSI).* Consists of three citizens elected by the *Assembleia da República* (national parliament) for a period of four years. the *Assemblea da República* can call both Directors of SIS and SIEDM to be heard before a parliamentary committee	Th co do al
PORTUGAL	**Serviço de Informações de Seguranca (SIS)** reports to the Minister of the Interior		security service for internal affairs; protecting the Constitution (no executive powers); collecting and evaluating intelligence on criminal and anti-State activities			

Country	Intelligence service	Legal basis	Duties	SIGINT capacity	Control authority	Le
SPAIN	**Centro Superior de Información de la Defensa (CESID)** reports to the Minister of Defence	*R.D. 2632/1985 de 27.12.1985 (BOE 20.01.1986) Estructura interna y relaciones del Centro Superior de la Defensa;* as amended by *R.D. 266/1996 de 16.02.1996 Modif. de la estructura organica del CESID*	foreign and internal intelligence service; procurement of political, economic, technological/scientific and military information; foreign intelligence coverage, counter-intelligence inside and outside Spain	yes	no specific control body; general parliamentary scrutiny by parliamentary committees as with other government authorities	
SPAIN	**Dirección General de la Guardia Civil (GC)** reports to the Minister of Defence and the Minister of the Interior	*L.Org. 2/1986 de 13.03.1986 (BOE 14.03.1986) de Fuerzas y cuerpos de seguridad*	Central Spanish paramilitary police authority including police intelligence service; fight against organised crime on Spanish territory			
SPAIN	**Dirección General de la Policia** reports to the Ministry of the Interior		Central Spanish police authority, including police intelligence service; internal and foreign intelligence relating to terrorist structures and Islamic fundamentalism in the Middle East and North Africa			

Country	Intelligence service	Legal basis	Duties	SIGINT capacity	Control authority	Le
SWEDEN	Säkerhetspolisen (SÄPO) Civilian Intelligence and Security Service reports to the Minister of Justice	*Polislag (1984:387) Förordning (1989:773) med instruktion för Rikspolisstyrelsen* 'Police Act (1984:387) Ordinance (1989:773) and Directive for the National Police Board'	Responsibilities: - Security control - Counter-intelligence - Counter-terrorism - Protection of the Constitution Staff during 1999 about 800. 1995 Budget SEK 475 million (EUR 55.7 million)		Control body of the NPB, consisting of five MPs, two members of staff and the National Police Commissioner. *Registernämnd*, which consists of a maximum of eight members. At the moment there are two law officers, two MPs, a lawyer and an expert. Both bodies report to the Government	*Fo* *m* *R* 'C ar Na *Fo* *m* *R* 'C ar Re

Country	Intelligence service	Legal basis	Duties	SIGINT capacity	Control authority	Le
SWEDEN	**Militära Underrättelse och Säkerhetstjänsten (MUST)** 'Military intelligence and security directorate'; Part of the Swedish military headquarters. military intelligence and security service reports to Minister of Defence	*Act 2000:130 and Ordinance 2000:131 on military intelligence service*	collection and analysis of secret military or political intelligence; counter-intelligence; counteracting subversion, sabotage and disorder; protecting the armed forces and arms industry		*Försvarets underrättelsenämnd* 'Defence Intelligence Control Commission', consists in part of MPs	*O w Fo ur M Co*
SWEDEN	**Försvarets Radioanstalt (FRA)** **independent special unit (radio station)**		military and non-military intelligence, decryption of communications; radar surveillance	yes		

Country	Intelligence service	Legal basis	Duties	SIGINT capacity	Control authority	Le
UNITED KINGDOM	**Government Communications Headquarters (GCHQ)** reports to the Foreign Secretary	*Intelligence Services Act 1994*	counter-intelligence/ overseas intelligence; SIGINT in the poltical, economic, scientific/technological and military fields	yes	*The Security Service Commissioner* is appointed by the Prime Minister and is either a serving or retired senior judge *The Investigatory PowersTribunal* *Intelligence and Security Committee* The Committee consists of nine members (House of Commons + House of Lords, none of whom may be a Minister of the Crown) appointed by the Prime Minister	*In Ac* *In Ac* *In Ac*
	Secret Intelligence Sevice (SIS) = MI6 reports to the Foreign Secretary	*Intelligence Services Act 1994*	gathering information on intelligence activities and political events abroad			

Country	Intelligence service	Legal basis	Duties	SIGINT capacity	Control authority	Le
UNITED KINGDOM	**Security Service = MI5**, reports to the Home Secretary	*Security Services Acts 1989 and 1996*	intelligence gathering to safeguard internal security; counter-intelligence, counteracting extremist movements (including the IRA), Terrorism, and subversive elements		*Security Service Commissioner* *Intelligence and Security Committee*	*Se 19* *In Ac*
UNITED KINGDOM	**Defence Intelligence Staff (DIS)** reports to the Minister of Defence		supporting military security; evaluating and analysing military, political, technical/scientific and selected economic information			

Country	Intelligence service	Legal basis	Duties	SIGINT capacity	Control authority	Le
USA	**Central Intelligence Agency (CIA)**	*National Security Act 1947*	world-wide intelligence gathering; counter-espionage abroad, central responsibility for all intelligence matters in the USA		*Senate*: S*enate Select Committee on Intelligence (SSCI)* *House of Representatives: House Permanent Select Committee on Intelligence (HPSCI)*	es ba de re *In Ac* H. 95 es ba of R 17 in *O*

USA	**Defense Intelligence Agency (DIA)**	established by the 1961 *Directive 5105.21* by the Defence Secretary *Executive Order 11905* of 1976 *DoD Directive 5105.21 1978 Executive Order 12036* *1981 Executive Order 12333*	responsible for supplying military intelligence für intervention forces and decision-makers in the Defence Ministry and in the Government		S*enate Select Committee on Intelligence (SSCI)* *House Permanent Select Committee on Intelligence (HPSCI*	se

Country	Intelligence service	Legal basis	Duties	SIGINT capacity	Control authority	Le
USA	**National Security Agency (NSA)**	*Executive Order 12333 of 4 December 1981*	responsible for the security of US Intelligence systems, especially decryption; responsible for interception of communications abroad	yes	*Senate Select Committee on Intelligence (SSCI)* *House Permanent Select Committee on Intelligence (HPSCI)*	se
USA	**National Imagery and Mapping Agency (NIMA)**	*National Imagery and Mapping Agency Act of 1996.*	responsible for supplying images and maps and for analysing them;		*Senate Select Committee on Intelligence (SSCI)* *House Permanent Select Committee on Intelligence (HPSCI)*	se
USA	**National Reconnaissance Office (NRO)**		responsible for the development and use of satellite espionage systems (SIGINT, images)		*Senate Select Committee on Intelligence (SSCI)* *House Permanent Select Committee on Intelligence (HPSCI)*	se

Country	Intelligence service	Legal basis	Duties	SIGINT capacity	Control authority	Le
USA	**US Army Intelligence (e.g. Deputy Chief of Staff for Intelligence), Intelligence and Security Command (INSCOM)**	*Executive Order 12333* (December 4,1981)	Intelligence gathering and analysis in the military sphere; development of concepts und systems for military intelligence und electronic warfare	yes	S*enate Select Committee on Intelligence (SSCI)* *House Permanent Select Committee on Intelligence (HPSCI)*	se
USA	**Marine Corps Intelligence Activity (MCIA) National Maritime Intelligence Center (NMIC)**	*Executive Order 12333* (December 4, 1981)	Naval intelligence; military reconnaissance and development of decryption and electronic warfare support systems	yes	S*enate Select Committee on Intelligence (SSCI)* *House Permanent Select Committee on Intelligence (HPSCI)*	se
USA	**Office of Naval Intelligence (ONI)**	*Executive Order 12333* (December 4, 1981)	intelligence für Navy and maritime issues, Analysis of foreign fleets, collecting data about ocean surveillance systems and about submarine platforms and weapons systems	yes	S*enate Select Committee on Intelligence (SSCI)* *House Permanent Select Committee on Intelligence (HPSCI)*	se

Country	Intelligence service	Legal basis	Duties	SIGINT capacity	Control authority	Le
USA	**Air Intelligence Agency (AIA)**	*Executive Order 12333* (December 4, 1981)	airforce intelligence for airforce, military reconnaissance	yes	S*enate Select Committee on Intelligence (SSCI)* *House Permanent Select Committee on Intelligence (HPSCI)*	se
USA	**Federal Bureau of Investigation (FBI)**	*Title 28, United States Code (U.S. Code)*, Section 533 established in 1908; under this name since 1935.	counter-intelligence federal police force;		S*enate Select Committee on Intelligence (SSCI)* *House Permanent Select Committee on Intelligence (HPSCI)*	se
USA	**Drug Enforcement Administration**	*Executive Order of July 1, 1973*	collecting intelligence about drugs and money-laundering abroad		S*enate Select Committee on Intelligence (SSCI)* *House Permanent Select Committee on Intelligence (HPSCI)*	se

Country	Intelligence service	Legal basis	Duties	SIGINT capacity	Control authority	Le
Canada	**Communication Security Establishment (CSE);** is supported by the **Canadian Forces Supplementary Radio System (CFSRS)**	Formal mandate constitutes classified information but is probably approved by the Cabinet	Advises government and business about security issues relating to data transmission and processing (Infosec), development of encryption systems	yes	no independent control authority (subject solely to monitoring by the Auditor General and the Minister of Defence who is accountable to Parliament)	(1 *Ac*
Canada	**Canadian Security Intelligence Service (CSIS)** reports to the Minister of the Interior	*Canadian Security Intelligence Service Act (CSIS Act)* aus 1984	counter-espionage, combating sabotage and international terrorism in Canada		**The Security Intelligence Review Committee (SIRC)** independent body consisting of 5 members who may not be Members of Parliament	*Ca* *In* *Ac*
Canada	**Director General Intelligence Division** (under the *Deputy Chief of the Defence Staff)* reports to the Minister of Defence		intelligence in the military sphere			

Country	Intelligence service	Legal basis	Duties	SIGINT capacity	Control authority	Le
Australia	**Defence Signals Directorate (DSD**) reports to the Minister of Defence		collecting and disseminating signals intelligence; supplying information security products (Infosec) for the Government and for the military		*Inspector General of Intelligence and Security (IGIS)* (appointed by the Prime Minister)	In In Se
Australia	**Defence Intelligence Organisation (DIO)** reports to the Minister of Defence		collecting and analysing strategic and military information und intelligence		*Inspector-General of Intelligence and Security (IGIS)*	se
Australia	**Australian Secret Intelligence Service (ASIS)** foreign intelligence service reports to the Foreign Minister		collecting foreign intelligence, with particular reference to South-East Asia in the interests of national security, business and external relations		*Inspector-General of Intelligence and Security (IGIS)*	se

Country	Intelligence service	Legal basis	Duties	SIGINT capacity	Control authority	Le
Australia	**Australian Security Intelligence Organisation (ASIO)**	*The Australian Security Intelligence Organisation Act 1979 (the ASIO Act)*	protection against politically motivated violence; personal and material security combating international terrorism and illegal technology transfer		*Parliamentary Joint Committee on the Australian Security Intelligence Organization* *Inspector-General of Intelligence and Security (IGIS)*	Se AS se
Australia	**Office of National Assessments** independent body	*Office of National Assessments Act 1977*	reports to the Prime Minister		*Inspector-General of Intelligence and Security (IGIS)*	se

Country	Intelligence service	Legal basis	Duties	SIGINT capacity	Control authority	Le
New Zealand	**Government Communications Security Bureau (GCSB)** reports to the Prime Minister	established in 1977 no legal basis to date, but a bill is currently before Parliament (*Government Communications Security Bureau Bill*)	securing information about foreign countries; communications security, computer and information security (Infosec); technical security	yes	*Inspector-General of Intelligence and Security* *Intelligence and Security Committee* (Prime Minister, Leader of the Opposition, 3 MPs)	*Th of Se* *Th Se Ac*
New Zealand	**New Zealand Security Intelligence Service (SIS)** internal intelligence service reports to the Prime Minister	*New Zealand Security Intelligence Service Act 1969*	counter-intelligence, protection against terrorism and politically motivated violence, raising awareness in scientific research and industry to the problems of industrial espionage and illegal technological transfer			
Country	**Intelligence service**	**Legal basis**	**Duties**	**SIGINT capacity**	**Control authority**	**Le**
New Zealand	**External Assessments Bureau (EAB)** foreign intelligence service reports to the Prime Minister		analyses political developments and draws up reports on political and economic events and trends			
New Zealand	**Directorate of Defence Intelligence and Security (DDIS)**		military intelligence service; collects data relevant to the military, above all in the Asia-Pacific			

	military intelligence service reports to the Minister of Defence		area; analysis of tactical and strategic information			

PARLEMENT EUROPÉEN

1999 *2004*

Document de séance

FINAL
A5-0264/2001
Partie 1

11 juillet 2001

RAPPORT

sur l'existence d'un système d'interception mondial des communications privées et économiques (système d'interception ECHELON) (2001/2098(INI))

Partie 1 Proposition de résolution
Exposé des motifs

Commission temporaire sur le système d'interception ECHELON

Rapporteur: Gerhard Schmid

"Sed quis custodiet ipsos custodes."

Juvenal (v. 60 – v. 130), Sat. 6, 347

SOMMAIRE

Page

PAGE RÉGLEMENTAIRE 11

PROPOSITION DE RÉSOLUTION 12

EXPOSÉ DES MOTIFS 23

1. Introduction 23

1.1. Motif de la constitution de la commission 23
1.2. Affirmations formulées dans les deux études du STOA sur un système d'interception mondial appelé ECHELON 23
1.2.1. Premier rapport du STOA de 1997 23
1.2.2. Rapports du STOA de 1999 23
1.3. Mandat de la Commission 24
1.4. Pourquoi n'avoir pas opté pour une commission d'enquête? 25
1.5. Méthodes et plan de travail 25
1.6. Caractéristiques attribuées au système ECHELON 26

2. Activité des services de renseignements extérieurs 28

2.1. Introduction 28
2.2. Que faut-il entendre par espionnage? 28
2.3. Objectifs de l'espionnage 28
2.4. Méthodes de l'espionnage 29
2.4.1. Recours à l'être humain dans l'espionnage 29
2.4.2. Exploitation des signaux électromagnétiques 30
2.5. Activité de certains services de renseignements 30

3. Conditions techniques minimales requises pour l'interception des télécommunications 32

3.1. Possibilité d'interception des différents supports des télécommunications 32
3.2. Possibilités d'interception sur place 32
3.3. Possibilités d'un système d'interception fonctionnant à l'échelle mondiale 33
3.3.1. Accès aux supports des télécommunications 33
3.3.2. Possibilités d'exploitation automatique des communications interceptées: utilisation de filtres 37
3.3.3. Exemple du service de renseignements allemand 38

4. Technique des communications satellitaires 40

4.1. Importance des satellites de télécommunications…… 40
4.2. Fonctionnement d'une liaison satellitaire……. 41
4.2.1. Satellites géostationnaires…… 41
4.2.2. Cheminement d'une liaison satellitaire de télécommunications…….. 41
4.2.3. Principaux systèmes de communications satellitaires existants…….. 42
4.2.3.1. Systèmes de satellites fonctionnant à l'échelle mondiale…..…… 43
4.2.3.2. Systèmes de satellites nationaux……..…… 45
4.2.3.3. Systèmes de satellites régionaux……..…… 46
4.2.4. Attribution de fréquences…… 46
4.2.5. Zones couvertes par les satellites (empreintes au sol)…… 47
4.2.6. Dimensions des antennes requises pour une station terrienne…… 48
4.3. Communications par satellites à finalités militaires…….…… 49
4.3.1. Généralités…….. 49
4.3.2. Fréquences utilisées par les militaires…… 49
4.3.3. Taille des stations de réception……...…… 49
4.3.4. Exemples...…….…. 49

5. Preuve par indices de l'existence d'au moins un système d'interception mondial…… 50

5.1. Pourquoi une preuve par indices…….. 50
5.1.1. Preuve de l'activité d'interception des services de renseignements étrangers.… 50
5.1.2. Preuve de l'existence de stations dans les zones géographiques requises……... 51
5.1.3. Preuve d'une association étroite entre les services de renseignement……..… 51
5.2. Comment reconnaît-on une station d'interception des communications par satellite?…… 51
5.2.1. Critère 1: accès de l'installation…….. 51
5.2.2. Critère 2: type d'antenne……. 52
5.2.3. Critère 3: dimension de l'antenne…… 52
5.2.4. Critères 4: Preuves officielles……. 53
5.3. Données pouvant être obtenues par chacun, concernant les stations d'interception connues…….. 53
5.3.1. Méthode……..…. 53
5.3.2. Analyse approfondie…… 54
5.3.2.1. Le parallélisme entre le développement des INTELSAT et la construction de stations…….. 54
5.3.2.2. La couverture globale par stations qui écoutent manifestement des satellites de communication……. 57
5.3.2.3. Les stations: détails…… 58
5.3.2.3.1. Stations destinées à l'écoute de satellites de communication……. 58
5.3.2.3.2. Autres stations…….……. 61
5.3.3. Résultats: résumé…..…….. 63
5.4. L'accord UKUSA……. 64
5.4.1. Genèse de l'accord UKUSA…… 64
5.4.2. Éléments attestant de l'existence de l'accord…….. 65
5.4.2.1. Rapport annuel 1999/2000 de la commission britannique du

renseignement et de la sécurité……. 65
5.4.2.2. Informations fournies par les services du Premier Ministre de Nouvelle- Zélande…… 66
5.4.2.3. Liste des acronymes utilisés par la Navy…….. 66
5.4.2.4. Déclaration du directeur du DSD…….. 66
5.4.2.5. Rapport du Canadian Parliamentary Security and Intelligence Committee…… 66
5.4.2.6. Déclaration de M. Louis Torella, ancien directeur adjoint de la NSA.. 66
5.4.2.7. Lettre de M. Joe Hooper, ancien directeur du GCHQ…… 67
5.4.2.8. Interlocuteurs du rapporteur…… 67
5.5. Exploitation des documents américains ayant cessé d'être classés confidentiels…….. 67
5.5.1. Nature des documents…….. 67
5.5.2. Contenu des documents……... 67
5.5.2.1. Mission et conception de la NSA (documents 1, 2b, 4, 10 et 16)…….. 68
5.5.2.2. Pouvoirs des services de renseignement (document 7)…….. 69
5.5.2.3. Coopération avec d'autres services (documents 2 a et 2 b)…… 69
5.5.2.4. Mention des unités actives sur les "sites ECHELON" (documents 9 et 12)…….. 69
5.5.2.5. Mention de stations (documents 6, 9 et 12, nouveaux documents)….. 69
5.5.2.6. Protection de la vie privée des citoyens américains (documents 7, 7 a à f, 9, 11 et 16)…… 70
5.5.2.7. Définitions (documents 4, 5 a et 7)…… 71
5.5.3. Résumé…… 71
5.6. Renseignements émanant d'auteurs spécialisés et de journalistes……. 72
Nicky Hager……..… 72
Duncan Campbell…….. 73
Jeff Richelson…… 74
James Bamford……..…. 75
Bo Elkjaer et Kenan Seeberg…… 76
5.7. Déclarations d'anciens collaborateurs des services de renseignement…….. 76
5.7.1. Margaret Newsham (ex-collaboratrice de la NSA)……... 76
5.7.2. Wayne Madsen (ancien collaborateur de la NSA)……. 77
5.7.3. Mike Frost (ancien collaborateur des services secrets canadiens)……. 77
5.7.4. Fred Stock (ancien collaborateur des services secrets canadiens)…… 78
5.8. Informations de sources gouvernementales……. 78
5.8.1. Déclarations américaines…… 78
5.8.2. Déclarations anglaises…… 79
5.8.3. Déclarations australiennes……..…… 79
5.8.4. Déclarations néo-zélandaises……..… 80
5.8.5. Déclarations néerlandaises……. 80
5.8.6. Déclarations italiennes……... 80
5.9. Questions au Conseil et à la Commission……..… 80
5.10. Rapports parlementaires……... 82
5.10.1. Rapports du comité permanent R de contrôle belge…….. 82
5.10.2. Rapport de la commission de la défense nationale de l'Assemblée nationale française…….. 82
5.10.3. Rapport de la commission du Parlement italien chargée des services de

renseignements et de sécurité ainsi que de la sûreté de l'État…… 83

6. Peut-il exister d'autres systèmes d'interception mondiaux?…….. 84

6.1. Conditions nécessaires pour un tel système …… 84
6.1.1. Conditions technico-géographiques……. 84
6.1.2. Conditions politico-économiques……..….. 84
6.2. France……... 84
6.3. Russie…….….. 85
6.4. Autres pays du G8 et Chine……. 86

7. Compatibilité d'un système d'interception des communications du type "ECHELON" avec le droit de l'Union européenne…… 87

7.1. Commentaires sur la question…….. 87
7.2. Compatibilité d'un système de renseignement avec le droit de l'Union européenne... 87
7.2.1. Compatibilité avec le droit communautaire……..... 87
7.2.2. Compatibilité avec d'autres dispositions législatives de l'Union européenne.. 88
7.3. Problème de la compatibilité en cas d'utilisation du système aux fins de l'espionnage économique……. 89
7.4. Conclusions…….. 90

8. La surveillance des communications par les services de renseignement est-elle compatible avec le droit fondamental au respect de la vie privée…….. 91

8.1. La surveillance des communications, atteinte au droit fondamental au respect de la vie privée…….. 91
8.2. La protection de la vie privée garantie par les conventions internationales…….. 91
8.3. Les dispositions de la convention européenne des droits de l'homme…….. 92
8.3.1. L'importance de la convention dans l'UE……..…… 92
8.3.2. Portée de la protection offerte par la convention…….…. 93
8.3.3. Surveillance des télécommunications au regard de l'article 8 de la convention 93
8.3.4. Importance de l'article 8 de la convention sous l'angle des activités des services de renseignements……..... 94
8.4. Obligation de vigilance vis-à-vis des activités de services de renseignements étrangers……..… 96
8.4.1. Caractère inadmissible d'une violation de l'article 8 de la convention liée à l'intervention de services de renseignements étrangers……..… 96
8.4.2. Conséquences sous l'angle des activités de services de renseignements extra-européens sur le territoire de pays signataires de la convention……... 96
8.4.2.1. Jurisprudence de la Cour européenne des droits de l'homme…….. 96
8.4.2.2. Conséquences en ce qui concerne les stations……..... 97
8.4.2.3. Conséquences en ce qui concerne les écoutes pratiquées sur instructions de l'étranger…….. 97
8.4.2.4. Obligation de vigilance par rapport aux pays tiers…… 97

9. Les citoyens de l'UE sont-ils suffisamment protégés face aux activités des services de renseignements? 99

9.1. Protection face aux activités des services de renseignements: rôle des parlements nationaux 99
9.2. Pouvoirs des autorités nationales en matière de mesures de surveillance 99
9.3. Les contrôles des services de renseignements 100
9.4. Analyse de la situation du citoyen européen 103

10. Protection contre l'espionnage économique 105

10.1. Économie et espionnage 105
10.1.1. Les objectifs de l'espionnage 105
10.1.1.1. Branches 105
10.1.1.2. Départements d'entreprise 105
10.1.2. Espionnage de concurrence 106
10.2. Les préjudices causés par l'espionnage 106
10.3. Qui espionne? 107
10.3.1. Collaborateurs de l'entreprise (délit d'initié) 107
10.3.2. Officines spécialisées 108
10.3.3. Hackers 108
10.3.4. Services de renseignements 108
10.4. Comment espionne-t-on? 108
10.5. Espionnage économique d'État 109
10.5.1. Espionnage économique stratégique effectué par les services de renseignements 109
10.5.2. Les services de renseignements, agents de l'espionnage de concurrence 109
10.5.2.1. Pays très avancés sur le plan technologique 109
10.5.2.2. Pays moins avancés sur le plan technique 109
10.6. ECHELON est-il adapté à l'espionnage industriel? 110
10.7. Cas divulgués 110
10.8. Protection contre l'espionnage économique 116
10.8.1. Protection juridique 116
10.8.2. Autres entraves à l'espionnage économique 116
10.9. Les États-Unis et l'économie après la guerre froide 117
10.9.1. Le défi lancé au gouvernement américain: l'espionnage économique contre les entreprises américaines 118
10.9.1.1. Les acteurs 119
10.9.1.2. Objectifs de l'espionnage économique 119
10.9.1.3. Méthodes 120
10.9.2. Attitude du gouvernement américain face à l'espionnage économique actif 120
10.9.3. Situation juridique en matière de corruption d'agents publics 121
10.9.4. Rôle de l'Advocacy Center dans la promotion des exportations américaines 123
10.9.4.1. Missions de l'Advocacy Center 123
10.9.4.2. Méthodes de travail 124
10.9.4.3. Participation de la CIA aux travaux du TPCC 124

10.9.4.4. Questions sans réponse…….. 125
10.10. Sécurité des réseaux informatiques…….. 125
10.10.1. Importance du présent chapitre…….. 125
10.10.2. Risque inhérent à l'utilisation de la technologie de l'information moderne dans les milieux économiques…….. 125
10.10.2.1. Augmentation du risque…… 126
10.10.2.2. Analyse détaillée de certains des risques…….. 126
10.10.3. Fréquence des attaques contre les réseaux……. 127
10.10.4. Acteurs et méthodes…….. 128
10.10.5. Piratage de l'extérieur…….... 129
10.11. Sous-estimation des risques……. 129
10.11.1. Conscience des risques dans les milieux économiques……. 129
10.11.2. Conscience du risque dans les milieux scientifiques……. 129
10.11.3. Conscience du risque dans les institutions européennes…… 130
10.11.3.1. Banque centrale européenne……. 130
10.11.3.2. Conseil de l'Union européenne……. 130
10.11.3.3. Parlement européen…….. 130
10.11.3.4 Commission européenne…….. 131

11. Le cryptage en tant qu'instrument d'autoprotection…….. 132

11.1. Objectif et mode de fonctionnement du cryptage…… 132

11.1.1. Objectif du cryptage……. 132
11.1.2. Mode de fonctionnement du cryptage…… 132
11.2. Sécurité des systèmes de cryptage…… 134
11.2.1. Généralités……. 134
11.2.2. Sécurité absolue: one-time pad…….. 134
11.2.3. Sécurité relative en fonction de l'état de la technique…… 134
11.2.3.1. Utilisation de machines de cryptage et de décryptage…… 134
11.2.3.2. Utilisation de l'ordinateur…… 135
11.2.4. Normalisation et limites de la sécurité…….. 135
11.3. Problème de sécurité en matière de diffusion des clés……. 136
11.3.1. Cryptage asymétrique: procédé de la public-key…….. 136
11.3.2. Cryptage par public-key pour les particuliers…… 137
11.3.3. Méthodes à venir…… 138
11.4. Sécurité des produits de cryptage……. 138
11.5. Cryptage et intérêts nationaux……. 138
11.5.1. Tentatives de limitation du cryptage……. 138
11.5.2. Importance d'un cryptage sûr pour le commerce électronique……. 139
11.5.3. Problème des hommes d'affaires en déplacement..... 139
11.6. Problèmes pratiques du cryptage…….. 139

12. Relations extérieures de l'UE et collecte de renseignements…….. 141

12.1. Introduction…….. 141
12.2. Possibilités de coopération au sein de l'UE…….. 141
12.2.1. La coopération actuelle……. 141

12.2.2. Avantages d'une politique commune dans le domaine du renseignement…… 142
12.2.2.1. Avantages pratiques…….. 142
12.2.2.2. Avantages financiers…….. 142
12.2.2.3. Avantages politiques…….. 142
12.2.3. Remarques finales……. 142
12.3. Coopération au-delà de l'Union…… 143
12.4. Remarques finales…… 144

13. Conclusions et recommandations……. 145

13.1. Conclusions…….. 145
13.2. Recommandations…… 149

L'OPINION MINORITAIRE ET LES ANNEXES SONT PUBLIÉES SÉPARÉMENT DANS LA PARTIE 2

PAGE RÉGLEMENTAIRE

Au cours de sa séance du 5 juillet 2000, le Parlement européen a décidé, conformément à l'article 150, paragraphe 2 de son règlement, de créer une commission temporaire sur le système d'interception ECHELON et de définir le mandat de celle-ci (v. chapitre 1, point 1.3 de l'exposé des motifs). Au cours de sa réunion constitutive du 6 juillet 2000, la commission temporaire a nommé Gerhard Schmid rapporteur.

Au cours de ses réunions des 29 mai, 20 juin et 3 juillet, elle a examiné le projet de rapport.

Au cours de la dernière de ces réunions, elle a adopté la proposition de résolution par 27 voix contre 5 et 2 abstentions.

Étaient présents au moment du vote Carlos Coelho, président, Elly Plooij-van Gorsel, Neil MacCormick et Giuseppe Di Lello Finuoli, vice-présidents, Gerhard Schmid, rapporteur, Mary Elizabeth Banotti, Bastiaan Belder, Maria Berger, Charlotte Cederschiöld, Gérard M.J. Deprez, Giorgos Dimitrakopoulos, Robert J.E. Evans, Colette Flesch, Pernille Frahm, Anna Karamanou, Eva Klamt, Alain Krivine, Torben Lund, Erika Mann, Jean-Charles Marchiani, Hugues Martin, Patricia McKenna, William Francis Newton Dunn, (suppléant Jorge Salvador Hernández Mollar conformément à l'article 153, paragraphe 2, du règlement), Reino Paasilinna, Bernd Posselt, (suppléant Hubert Pirker), Jacques Santkin (suppléant Catherine Lalumière), Ilka Schröder, Gary Titley (suppléant Ozan Ceyhun), Maurizio Turco, Gianni Vattimo, W.G. van Velzen, Christian von Bötticher, Jan Marinus Wiersma, Christos Zacharias (suppléant Enrico Ferri).

L'opinion minoritaire et les annexes sont publiées séparément (A5-0264/2001-Par2).

Le rapport a été déposé le 11 juillet 2001.

Le délai de dépôt des amendements sera indiqué dans le projet d'ordre du jour de la période de session au cours de laquelle le rapport sera examiné.

PROPOSITION DE RÉSOLUTION

Résolution du Parlement européen sur l'existence d'un système d'interception mondial des communications privées et économiques (système d'interception ECHELON) (2001/2098 (INI))

Le Parlement européen,

– vu sa décision du 5 juillet 2000, relative à la création d'une commission temporaire sur le système d'interception ECHELON, ainsi que le mandat de ladite commission[1],

– vu le traité CE, qui vise la mise en place d'un marché commun présentant un degré élevé de compétitivité,

– vu les articles 11 et 12 du traité sur l'Union européenne qui lient les Etats membres à l'obligation de renforcer et développer leur solidarité politique mutuelle,

– vu le traité sur l'Union européenne, en particulier l'article 6, paragraphe 2, de celui-ci, qui prévoit l'obligation de respecter les droits fondamentaux, ainsi que le titre V dudit traité, qui reprend les dispositions concernant une politique étrangère et de sécurité commune,

– vu l'article 12 de la Déclaration universelle des droits de l'homme,

– vu la Charte des droits fondamentaux de l'UE, dont l'article 7 garantit le respect de la vie privée et familiale et prévoit le droit au respect des communications et l'article 8 protège les données à caractère personnel,

– vu la Convention européenne relative aux droits de l'homme, en particulier l'article 8 de celle-ci, qui protège la vie privée et la confidentialité des correspondances, ainsi que les nombreux autres traités internationaux qui protègent la vie privée,

– vu les travaux de la commission temporaire sur le système d'interception Echelon, qui a tenu de nombreuses auditions et réunions avec les experts les plus divers, en particulier avec des responsables des secteurs public et privé dans les domaines des télécommunications et de la protection des données, avec des membres des services de renseignements, des journalistes, des avocats experts en la matière, des députés des parlements des États membres, etc.,

– vu l'article 150, paragraphe 2, de son règlement,

– vu le rapport de la commission temporaire sur le système d'interception ECHELON (A5-0264/2001),

[1] JO C 121 du 24.4.2001, p. 36.

en ce qui concerne l'existence d'un système d'interception mondial des communications privées et économiques (système d'interception ECHELON)

A. considérant que l'existence d'un système d'interception mondial des communications fonctionnant avec la participation des États-Unis, du Royaume-Uni, du Canada, de l'Australie et de la Nouvelle-Zélande, dans le cadre de l'accord UKUSA, ne fait plus de doutes; qu'il apparaît vraisemblable, eu égard aux indices disponibles et à de nombreuses déclarations concordantes provenant d'horizons très divers – y compris de sources américaines – , que l'on peut penser que le système ou certaines parties de celui-ci portaient, du moins pendant quelque temps, le nom de code ECHELON,

B. considérant qu'il est incontestable qu'il est utilisé au moins pour intercepter des communications privées et économiques, mais non militaires, et que l'analyse menée dans le cadre du rapport a montré que la capacité technique de ce système n'est peut être pas aussi grande, tant s'en faut, que ce que certains médias ont supposé,

C. considérant qu'il est dès lors étonnant, voire inquiétant, que de nombreux responsables communautaires auditionnés, notamment des commissaires européens, aient déclaré ne pas avoir connaissance de ce phénomène,

en ce qui concerne les limites du système

D. considérant que le système de surveillance repose notamment sur l'interception de communications par satellite, mais que, dans les régions à forte densité de communications, seule une très modeste partie des communications s'effectue par satellite; que la majeure partie des communications ne peuvent être interceptées par des stations au sol mais uniquement par branchement sur câble ou par écoute radio, ce qui, comme les investigations effectuées dans le cadre du rapport l'ont montré, n'est possible que dans des limites très étroites; que le personnel nécessaire pour analyser les communications interceptées détermine d'autres limites, que les pays membres d'UKUSA n'ont, par conséquent, accès qu'à une partie très restreinte des communications par câble ou par radio et ne peuvent en évaluer qu'une partie encore plus limitée, considérant également que, aussi importants que soient les moyens et la capacité existants pour pouvoir intercepter les communications, il est impossible dans la pratique, eu égard au nombre très élevé de celles-ci, de toutes les contrôler de manière exhaustive et détaillée,

en ce qui concerne l'existence d'autres systèmes d'interception

E. étant donné que l'interception des communications est un moyen d'espionnage traditionnel des services de renseignements et qu'un tel système pourrait être exploité par d'autres pays à condition qu'ils disposent des moyens financiers et des conditions géographiques nécessaires***;*** que la France est le seul État membre de l'UE qui, grâce à ses territoires d'outre-mer, serait en mesure, des points de vue géographique et technique, d'exploiter de manière autonome un système d'interception mondial et qu'elle possède aussi l'infrastructure technique et organisationnelle nécessaire pour ce faire; qu'il existe de très nombreux indices prouvant que la Russie exploite vraisemblablement aussi un tel système,

en ce qui concerne la compatibilité avec le droit de l'UE

F. considérant que, s'agissant de la compatibilité d'un tel système avec le droit de l'UE, il y a lieu de distinguer deux cas: si ledit système n'est utilisé qu'à des fins de renseignements, il n'y a aucune contradiction avec le droit de l'UE, dans la mesure où les activités qui relèvent de la sécurité de l'État ne sont pas couvertes par le traité CE mais ne relèvent que des titres V du traité UE (PESC), qui ne contient encore aucune disposition en la matière, de sorte qu'une base fait défaut. En revanche, si le système est utilisé de manière abusive pour espionner la concurrence, il y a manquement à l'obligation de loyauté et atteinte à l'idée d'un marché commun où la concurrence est libre; si un État membre participe à une telle démarche, il viole le droit de l'Union,

G. considérant les déclarations faites par le Conseil lors de la séance plénière du 30 mars 2000, selon lesquelles : "le Conseil ne peut accepter la création ou l'existence d'un système d'interception des télécommunications qui ne respecte pas les règles de droit des Etats membres et qui viole les principes fondamentaux visant à préserver la dignité humaine";

en ce qui concerne la compatibilité avec le droit fondamental au respect de la vie privée (article 8 de la Convention relative aux droits de l'homme)

H. considérant que toute interception de communication constitue une atteinte grave à la vie privée, que l'article 8 de la Convention relative aux droits de l'homme, qui protège la vie privée, n'autorise que des ingérences destinées à sauvegarder la sécurité nationale, à condition que le droit national prévoie les dispositions afférentes, que celles-ci soient accessibles à tous et déterminent les circonstances et conditions d'intervention de la puissance publique, que les ingérences doivent en outre être proportionnées, ce qui suppose une mise en balance des intérêts, et que, en vertu de la jurisprudence de la Cour des droits de l'homme, il ne suffit pas qu'elles soient opportunes ou souhaitables,

I. considérant qu'un système de renseignements qui intercepterait de manière aléatoire et en permanence les communications serait contraire au principe de proportionnalité et incompatible avec la Convention relative aux droits de l'homme, que, dans le même ordre d'idées, il y aurait violation de ladite Convention si les dispositions en vertu desquelles la surveillance des communications s'effectue sont dépourvues de base légale, si celle-ci n'est pas accessible à tous ou si elle est formulée de telle manière que la personne ne peut en appréhender les conséquences ou si l'atteinte n'était pas proportionnée***;*** que les dispositions sur la base desquelles des services de renseignements américains opèrent à l'étranger sont en grande partie confidentielles, de sorte que le respect du principe de proportionnalité est à tout le moins douteux et qu'il y a manquement au principe d'accès au droit et de prévisibilité de ses effets énoncé par la Cour des droits de l'homme,

J. considérant que les États membres ne peuvent se soustraire aux obligations qui leur incombent au titre de la Convention relative aux droits de l'homme en faisant intervenir sur leur territoire les services de renseignements d'autres pays soumis à des dispositions moins rigoureuses car cela reviendrait à priver de ses effets le principe de légalité et ses deux composantes – accès au droit et prévisibilité de ses effets – et viderait de sa substance la jurisprudence de la Cour des droits de l'homme,

K. considérant que la conformité des activités légales de services de renseignements avec les

droits fondamentaux suppose en outre que soient prévus des systèmes de contrôle suffisants parant au risque que comporte l'action secrète d'une partie de l'administration; que la Cour européenne des droits de l'homme a souligné expressément l'importance d'un système de contrôle efficace dans le domaine des activités des services de renseignements, ce qui fait qu'il apparaît préoccupant que certains États membres ne disposent pas d'organe de contrôle parlementaire de leurs services secrets,

en ce qui concerne la question de savoir si les citoyens de l'UE sont suffisamment protégés face aux services de renseignements

L. considérant que la protection des citoyens de l'UE dépend des situations juridiques qui existent dans les États membres, lesquelles sont très différentes et, dans certains cas, caractérisées par l'absence d'organe de contrôle parlementaire, ce qui fait que l'on ne saurait parler de protection suffisante; que les citoyens européens tiennent absolument à ce que leurs parlements nationaux disposent d'un organe de contrôle dûment et spécialement structuré pour surveiller et contrôler les activités des services de renseignements; que, même dans les pays où il existe un organe de contrôle, la tentation est grande de s'intéresser davantage aux activités intérieures des services de renseignements qu'à leurs activités extérieures, étant donné que, normalement, les citoyens du pays ne sont concernés que dans le premier cas***;*** considérant que le fait d'obliger les services de renseignements à informer un citoyen a posteriori, par exemple cinq ans après l'interception, que ses communications ont été interceptées, encouragerait des pratiques d'interception proportionnée,

M. considérant que, compte tenu de leur dimension, des stations de réception satellitaire ne peuvent être construites sur le territoire d'un pays sans son assentiment,

N. considérant qu'en cas de coopération entre services de renseignements dans le cadre de la PESC ou de la JAI, les institutions seraient appelées à mettre en place des dispositions de protection suffisantes pour les citoyens européens,

en ce qui concerne l'espionnage économique

O. considérant qu'il relève des missions des services de renseignements à l'étranger de s'intéresser aux données économiques telles que développement de branches, évolution du marché des matières premières, respect d'embargos, respect des dispositions relatives à l'approvisionnement en biens à usage mixte, etc., et que c'est la raison pour laquelle les entreprises exerçant des activités dans ces domaines sont fréquemment surveillées,

P. considérant que les services de renseignements des États-Unis s'occupent non seulement de problèmes économiques généraux mais aussi qu'ils interceptent des communications d'entreprises dans le contexte de passation de marchés, justifiant cela en invoquant la lutte contre les tentatives de corruption, que cette pratique porte en elle le risque que des informations soient utilisées non pas pour lutter contre la corruption mais à des fins d'espionnage concurrentiel même si les États-Unis affirment ne pas pratiquer celui-ci; que le rôle de l'Advocacy Center du ministère américain du commerce n'est toujours pas absolument clair et qu'un entretien avec cet organisme, qui devait contribuer à la clarification, a été refusé,

Q. considérant qu'une convention en matière de lutte contre la corruption de fonctionnaire a été adoptée en 1997 dans le cadre de l'OCDE, laquelle prévoit que la corruption est passible de sanctions internationales, de sorte que dans les cas d'espèce la corruption ne saurait justifier l'interception de communications,

R. considérant qu'il est toutefois intolérable que des services de renseignements soient utilisés pour l'espionnage de concurrence, espionnant des entreprises étrangères pour procurer des avantages concurrentiels aux entreprises nationales, mais qu'il n'est pas prouvé, même si cela est souvent avancé, que le système d'interception mondial soit utilisé à cette fin,

S. considérant que, lors de la visite effectuée aux États-Unis par une délégation de la commission temporaire, des sources autorisées ont confirmé le rapport Brown, indiquant que 5 % des informations collectées grâce à des sources non publiques sont utilisées à des fins économiques; que les mêmes sources estiment que cette surveillance pourrait permettre aux entreprises des États-Unis d'emporter jusqu'à 7 milliards de dollars de marchés,

T. considérant que les données sensibles se trouvent principalement à l'intérieur des entreprises, de sorte que l'espionnage consiste notamment à tenter d'obtenir des informations par le truchement de leurs collaborateurs ou de personnes infiltrées et, de plus en plus, en pénétrant dans les réseaux informatiques, que ce n'est que lorsque les données sensibles sont acheminées vers l'extérieur par câble ou par radio (satellite), qu'un système de surveillance des communications peut être utilisé pour espionner, trois cas pouvant se présenter:

- entreprises travaillant dans trois zones horaires, de sorte que les résultats intérimaires peuvent être envoyés d'Europe en Amérique puis en Asie,

- vidéoconférences d'entreprises multinationales se déroulant par satellite ou par câble,

- négociations de marchés importants sur place (construction d'usines, d'infrastructures de télécommunications, de systèmes de transport, etc.) lorsqu'il faut en référer à la maison mère à partir du site sur place,

U. considérant que, d'une manière générale, les petites et moyennes entreprises n'ont pas suffisamment conscience des risques et de la sécurité et ne reconnaissent pas les dangers de l'espionnage économique et de l'interception des communications,

V. considérant que le sens de la sécurité n'est pas toujours très développé dans les institutions européennes (hormis à la Banque centrale européenne, à la direction générale des relations extérieures du Conseil et à la direction générale des relations extérieures de la Commission), et qu'il y a donc lieu d'agir,

en ce qui concerne les possibilités de protection

W. considérant que la sécurité des entreprises ne peut être assurée qu'en protégeant l'ensemble de l'environnement de travail ainsi que tous les moyens de communication servant à transmettre des informations sensibles, que les systèmes de cryptage sûrs à prix abordable sont suffisamment nombreux sur le marché européen, que les particuliers doivent, eux

aussi, être engagés à crypter leur courrier électronique, un courrier non crypté s'assimilant à une lettre sans enveloppe, que, sur Internet, on trouve des systèmes conviviaux qui sont mis à la disposition des particuliers, parfois même gratuitement,

en ce qui concerne la coopération entre services de renseignements de l'UE

X. considérant que l'UE est convenue de coordonner la collecte du renseignement dans le cadre du développement d'une politique de sécurité et de défense tout en poursuivant la coopération avec d'autres partenaires dans ces domaines,

Y. considérant que le Conseil européen a décidé en décembre 1999 à Helsinki de se doter d'une capacité militaire européenne plus efficace afin de pouvoir s'acquitter de l'ensemble des missions de Petersberg dans le contexte de la PESC; qu'il a en outre décidé que, pour atteindre cet objectif d'ici à 2003, l'Union devait être en mesure de déployer rapidement des troupes d'environ 50 à 60 000 hommes qui seraient autonomes, disposant des capacités de commandement, de contrôle et de renseignements nécessaires; que les premiers pas dans la voie de la mise en place d'une telle capacité autonome en matière de renseignements ont déjà été franchis dans le cadre de l'UEO et du comité politique et de sécurité,

Z. considérant qu'une coopération entre services de renseignements de l'UE apparaît souhaitable car, d'une part, une politique commune de sécurité excluant les services secrets serait absurde et, d'autre part, cela comporterait de nombreux avantages d'ordre professionnel, financier et politique, que cela serait en outre conforme à l'idée d'un partenariat à égalité de droits avec les États-Unis et pourrait regrouper l'ensemble des États membres au sein d'un système mis sur pied dans le respect de la Convention des droits de l'homme; qu'un contrôle par le Parlement européen devrait, dans ce cas, être assuré,

AA. considérant que le Parlement européen est sur le point de se doter de dispositions relatives à l'accès aux informations et documents confidentiels et sensibles,

en ce qui concerne la conclusion et la modification de traités internationaux en matière de protection des citoyens et des entreprises

1. affirme, sur la base des informations recueillies par la commission temporaire que l'existence d'un système d'interception mondial des communications fonctionnant avec la participation des Etats-Unis, du Royaume-Uni, du Canada, de l'Australie et de la Nouvelle-Zélande, dans le cadre de l'accord UKUSA, ne fait plus de doute;

2. invite le Secrétaire général du Conseil de l'Europe à proposer au comité des ministres de déterminer s'il serait opportun d'adapter la protection de la vie privée garantie à l'article 8 de la Convention relative aux droits de l'homme aux méthodes de communication et aux possibilités d'interception modernes, et ce dans un protocole additionnel ou dans le contexte de la réglementation relative à la protection des données, dans le cadre d'une révision de la Convention afférente, étant entendu que cela ne saurait déboucher sur un abaissement du niveau de protection assuré par la Cour des droits de l'homme ni sur une réduction de la souplesse nécessaire pour suivre l'évolution;

3. demande aux États membres dont les dispositions législatives réglementant le pouvoir d'interception des services secrets créent des discriminations en matière de protection de la

vie privée de garantir à tous les citoyens européens les mêmes garanties légales en ce qui concerne la protection de la vie privée et la confidentialité de la correspondance;

4. invite les États membres de l'Union européenne à mettre en place une plate-forme européenne appelée à examiner les dispositions relatives à la garantie du secret de la correspondance et des communications, à se mettre d'accord sur un texte commun garantissant la protection de la vie privée, telle qu'elle est définie à l'article 7 de la Charte européenne des droits fondamentaux, à tous les citoyens européens sur le territoire des États membres et garantissant en outre que les activités des services de renseignements s'effectuent dans le respect des droits fondamentaux et, partant, des conditions énoncées au chapitre 8 du rapport, en particulier du point 8.3.4, en vertu de l'article 8 de la Convention relative aux droits de l'homme;

5. invite les États membres à adopter, lors de la prochaine conférence intergouvernementale, la Charte des droits fondamentaux en tant qu'instrument contraignant et pouvant faire l'objet de recours afin d'améliorer le niveau de protection des droits fondamentaux, notamment en ce qui concerne la vie privée;

6. invite les États membres du Conseil de l'Europe à adopter un protocole additionnel permettant à l'Union d'adhérer à la Convention relative aux droits de l'homme ou d'envisager d'autres moyens d'éviter les conflits de jurisprudence entre la Cour européenne des droits de l'homme et la Cour de justice européenne;

7. demande, en attendant, aux institutions de l'Union européenne, dans le cadre de leur sphère de compétence et d'action respective, de mettre en application les droits fondamentaux établis par la Charte;

8. invite le Secrétaire général des Nations unies à charger l'organe compétent de l'Organisation de présenter des propositions visant à adapter l'article 17 de la Convention internationale relative aux droits civils et politiques, qui garantit la protection de la vie privée, aux innovations techniques;

9. estime nécessaire la négociation et la signature d'une convention entre l'Union européenne et les Etats-Unis établissant que chacune des deux parties respecte à l'égard de l'autre les dispositions de protection de la vie privée des citoyens et de confidentialité des communications des entreprises applicables à ses propres citoyens et entreprises;

10. invite les États-Unis à signer le protocole additionnel à la Convention internationale relative aux droits civils et politiques afin de rendre possibles, en cas de violation, les recours individuels devant la commission des droits de l'homme prévue par la Convention; invite les ONG américaines compétentes, notamment l'ACLU (American Civil Liberties Union) et l'EPIC (Electronic Privacy Information Center) à faire pression en ce sens sur le gouvernement américain;

en ce qui concerne l'action législative nationale en matière de protection des citoyens et des entreprises

11. demande instamment aux États membres de vérifier la conformité aux droits fondamentaux, tels qu'ils sont définis dans la convention relative aux droits de l'homme et dans la jurisprudence de la Cour des droits de l'homme, de leur législation relative aux activités des services de renseignements et, au besoin, de lui apporter les adaptations nécessaires;

12. invite les Etats membres à se doter d'instruments contraignants garantissant une protection effective des personnes physiques et morales contre toute forme d'interception extralégale de leurs communications;

13. invite les États membres à rechercher un niveau uniforme de protection vis-à-vis des activités des services de renseignements et, à cette fin, à élaborer un code de conduite (voir paragraphe 4) en fonction du niveau de protection national le plus élevé, les citoyens concernés par les activités d'un service de renseignements étranger appartenant généralement à un autre pays, c'est-à-dire aussi à un autre État membre;

14. invite les États membres à négocier avec les États-Unis un code de conduite analogue à celui de l'UE;

15. invite les Etats membres qui ne l'ont pas encore fait à garantir un contrôle parlementaire et juridictionnel adéquat de leurs services secrets;

16. invite le Conseil et les États membres à mettre en place d'urgence un système de contrôle démocratique de la capacité de renseignements européenne autonome ainsi que des autres activités de renseignements communes ou coordonnées au niveau européen; suggère que le Parlement européen joue un rôle important dans ce système de contrôle;

17. invite les Etats membres à mettre en commun leurs moyens d'interception des communications afin de renforcer l'efficacité de la PESD dans les domaines du renseignement, de la lutte contre le terrorisme, la prolifération nucléaire ou le trafic international de stupéfiants, dans le respect des dispositions de protection de la vie privée des citoyens et de confidentialité des communications des entreprises, sous le contrôle du Parlement européen, du Conseil et de la Commission;

18. invite les États membres à conclure avec les pays tiers une convention visant à renforcer la protection de la vie privée des citoyens de l'Union, convention dans laquelle toutes les parties s'engagent à ce que, en cas d'interception pratiquée par l'une d'entre elles dans un autre pays signataire, la première informe ce dernier des actions envisagées;

en ce qui concerne les mesures de lutte contre l'espionnage économique

19. invite les États membres à examiner si des dispositions du droit européen et international permettraient de lutter contre l'espionnage économique et la corruption visant à obtenir des marchés, notamment si une réglementation dans le cadre de l'OMC serait possible, qui tiendrait compte des distorsions de concurrence causées par de telles pratiques, par exemple en prévoyant la nullité de tels marchés; invite les États-Unis, l'Australie, la Nouvelle-Zélande et le Canada à se joindre à cette initiative;

20. invite les Etats membres à s'engager à inclure dans le traité CE une clause interdisant

l'espionnage économique et à ne pas pratiquer l'espionnage économique entre eux, directement ou sous couvert d'une puissance étrangère qui pourrait intervenir sur leur sol, et à ne pas autoriser une puissance étrangère à mener des activités d'espionnage à partir du territoire d'un État membre de l'Union, afin de respecter l'esprit et la lettre du traité CE;

21. invite les États membres à s'engager, au moyen d'un instrument clair et contraignant, à ne pas pratiquer l'espionnage économique, proclamant ainsi le respect de l'esprit et de la lettre du traité CE; demande aux États membres de transposer ce principe contraignant dans leur législation nationale régissant les services de renseignements;

22. invite les États membres et le gouvernement des États-Unis à nouer un dialogue franc sur la collecte de renseignements économiques;

en ce qui concerne l'application du droit et le contrôle de celle-ci

23. lance un appel aux parlements nationaux qui ne disposent pas d'organe de contrôle parlementaire des services de renseignements pour qu'ils se dotent d'un tel organe;

24. invite les organes de contrôle nationaux des services secrets à accorder une grande importance, dans l'exercice de leur pouvoir de contrôle, à la protection de la vie privée, que la surveillance concerne les ressortissants nationaux, les citoyens d'autres États membres de l'UE ou ceux de pays tiers;

25. invite les États membres à s'assurer que leurs dispositifs de renseignements ne sont pas utilisés abusivement pour collecter des renseignements dans le cadre de la concurrence, au mépris de l'obligation de loyauté des États membres ainsi que de l'idée d'un marché unique fondé sur la libre concurrence;

26. invite l'Allemagne et le Royaume-Uni à subordonner l'autorisation d'interception, sur leur territoire, de communications par les services de renseignements des États-Unis à la condition que cela se fasse dans le respect de la Convention relative aux droits de l'homme, c'est-à-dire conformément au principe de proportionnalité, que la base juridique soit accessible et que les effets soient prévisibles pour les personnes et qu'un contrôle efficace soit prévu, étant donné qu'ils sont responsables de la conformité avec les droits de l'homme des activités de renseignements autorisées ou tolérées sur leur territoire;

en ce qui concerne la promotion de la protection des citoyens et des entreprises

27. invite la Commission et les États membres à informer les citoyens et les entreprises qu'il est possible que leurs communications internationales soient, dans certaines circonstances, interceptées; demande instamment que cette information s'assortisse d'une assistance pratique en matière de conception et de mise en œuvre de mesures de protection globales, englobant la sécurité des techniques d'information;

28. invite la Commission, le Conseil et les États membres à élaborer et à appliquer une politique efficace et active en matière de sécurité de la société de l'information; demande instamment que, dans le cadre de cette politique, une attention particulière soit accordée à la sensibilisation de tous les utilisateurs des systèmes de communication modernes en ce

qui concerne la protection des informations confidentielles; demande en outre que soit mis en place un réseau européen coordonné d'organismes capables de fournir une assistance pratique en matière de conception et de mise en œuvre de stratégies de protection globale;

29. invite la Commission et les États membres à élaborer des mesures de promotion, de développement et de fabrication de matériels et de logiciels de cryptage européens et surtout à soutenir les projets visant à développer des logiciels de cryptage conviviaux dont le texte-source soit publié;

30. invite la Commission et les États membres à promouvoir des projets de logiciels dont le texte-source soit publié, étant donné qu'il s'agit là de la seule manière de garantir qu'ils ne comportent pas de "backdoors" ("open-source software");

31. invite la Commission et les États membres à promouvoir des projets de logiciels dont le texte-source soit publié, étant donné qu'il s'agit là de la seule manière de garantir qu'ils ne comportent pas de "backdoors" ("open-source software"); invite la commission à définir une qualification du niveau de sécurité des logiciels destinés à l'échange de correspondances électroniques en plaçant les logiciels dont le code source n'est pas publié dans la catégorie la moins fiable;

32. invite les institutions européennes et les administrations publiques des États membres à recourir systématiquement au cryptage du courrier électronique afin de faire de celui-ci la règle, à terme;

33. invite les institutions communautaires et les administrations publiques des États membres à prévoir la formation de leur personnel et la familiarisation de celui-ci avec les nouvelles technologies et les techniques de cryptage en organisant les stages et les cours de formation nécessaires;

34. demande que la situation des pays candidats fasse l'objet d'une attention particulière; demande que ceux-ci soient aidés s'ils ne sont pas en mesure de se doter des moyens de protection nécessaires faute d'indépendance technologique;

en ce qui concerne d'autres démarches

35. invite les entreprises à coopérer davantage avec les services de contre-espionnage, à leur signaler les attaques extérieures relevant de l'espionnage économique, afin d'accroître leur efficacité;

36. invite la Commission à faire réaliser une analyse de sécurité destinée à préciser ce qui doit être protégé et à faire élaborer un schéma de protection;

37. invite la Commission à actualiser son système de cryptage, une modernisation s'imposant d'urgence, et demande à l'autorité budgétaire (Conseil et Parlement) de prévoir les moyens financiers à cette fin;

38. invite sa commission compétente à élaborer un rapport d'initiative sur la sécurité et la protection du secret dans les institutions européennes;

39. invite la Commission à assurer la protection des données dans le contexte du traitement

interne de celles-ci et à renforcer la protection des documents non accessibles au public;

40. invite la Commission et les États membres à investir, dans le cadre du 6e programme de recherche, dans les nouvelles technologies de cryptage et de décryptage;

41. demande qu'en cas de distorsion de concurrence due à des aides d'État ou à un recours abusif à l'espionnage économique, les États préjudiciés informent les autorités et les organes de contrôle de l'État d'origine de ces activités pour qu'il soit mis fin à celles-ci;

42. invite la Commission à proposer la création, en coopération étroite avec les entreprises et les États membres, d'un réseau européen et coordonné de centres de conseil, notamment dans les États membres qui ne possèdent pas de tels organes, en matière de sécurité de l'information dans les entreprises qui, à côté de la sensibilisation, aurait pour mission d'apporter une aide pratique;

43. estime opportun d'organiser un colloque non limité à l'Union sur la protection de la vie privée face à la surveillance des télécommunications afin de créer une plate-forme permettant aux ONG d'Europe, des États-Unis et d'autres pays d'examiner les aspects transfrontaliers et internationaux et de coordonner les activités et démarches;

44. charge sa Présidente de transmettre la présente résolution au Conseil et à la Commission, ainsi qu'au secrétaire général et à l'Assemblée parlementaire du Conseil de l'Europe, aux gouvernements et aux parlements des États membres et des pays candidats, des États-Unis, d'Australie, de Nouvelle-Zélande et du Canada.

EXPOSÉ DES MOTIFS

1. Introduction

1.1. Motif de la constitution de la commission

Le 5 juillet 2000, le Parlement a décidé de constituer une commission temporaire sur le système ECHELON. À la base de sa décision, le débat auquel donnait lieu l'étude que le STOA[2] avait commandée sur le système appelé ECHELON[3] et que son auteur, Duncan Campbell, avait présentée à l'occasion d'une audition de la commission des libertés et des droits des citoyens, de la justice et des affaires intérieures ayant pour thème l'Union européenne et la protection des données.

1.2. Affirmations formulées dans les deux études du STOA sur un système d'interception mondial appelé ECHELON

1.2.1. Premier rapport du STOA de 1997

Dans un rapport ayant pour thème l'évaluation des techniques de contrôle politique, dont le STOA avait, au nom du Parlement européen, confié en 1997 la réalisation à la Fondation Omega, une description du système ECHELON est aussi proposée au chapitre "Réseaux nationaux et internationaux d'interception des communications". L'auteur de l'étude y affirme que toutes les communications électroniques, téléphoniques et par fax en Europe sont quotidiennement interceptées par la NSA (Service américain de renseignement extérieur)[4]. Ce rapport a attiré l'attention de toute l'Europe sur l'existence d'ECHELON, réputé être un système d'interception polyvalent à l'échelle mondiale.

1.2.2. Rapports du STOA de 1999

Pour en apprendre davantage sur ce thème, le STOA commanda en 1999 une étude en cinq parties, portant sur le développement des techniques de surveillance et les risques d'utilisation abusive d'informations économiques. Le volume 2/5, qui est de la main de Duncan Campbell, est consacré à l'étude des capacités de renseignement actuelles et en particulier du fonctionnement d'ECHELON[5].

---

[2] STOA (Évaluation des choix scientifiques et techniques), service de la Direction générale des études du Parlement européen qui confie des travaux de recherche à l'extérieur, à la demande des commissions. Les études ne font pas l'objet d'une vérification scientifique.

[3] *Duncan Campbell*, The state of art in communications intelligence (COMINT) of automated processing for intelligence purposes of intercepting broadband multilanguage leased or common carrier system, and its applicability to COMINT argeting and selection, including speech recognition dans PE 168.184 (octobre 1999).

[4] *Steve Wright*, Une évaluation des techniques de contrôle politique, étude intérimaire STOA, PE 166.499 (1998), p. 20.

[5] *Duncan Campbell*, Der Stand der Dinge der Fernmeldeaufklärung (COMINT) in der automatisierten Verarbeitung zu nachrichtendienstlichen Zwecken von überwachten mehrsprachigen Breitbandmietleitungssystemen und den öffentlichen Leitungsnetzen und die Anwendbarkeit auf die Zielbestimmung und -auswahl von COMINT einschließlich der Spracherkennung, dans PE 168.184 (octobre 1999).

Une affirmation contenue dans ce rapport devait susciter un émoi particulier: ECHELON ne poursuivrait plus l'objectif qui était le sien au départ, à savoir la défense contre l'Est, et serait désormais un instrument d'espionnage économique. Cette thèse est étayée dans le rapport par des exemples d'espionnage économique présumés, qui auraient été la cause de préjudices notamment pour Airbus et Thomson CFS. Campbell s'appuie sur des informations fournies par la presse américaine[6].

À la suite de l'étude du STOA, ECHELON a fait l'objet de discussions dans quasiment tous les parlements des États membres; en France et en Belgique, des rapports ont même été établis à ce sujet.

1.3. Mandat de la commission

Par sa décision portant constitution d'une commission temporaire, le Parlement européen a également fixé son mandat[7]. Aux termes de celui-ci, la commission temporaire est chargée de:

" - vérifier l'existence du système d'interception des communications connu sous le nom d'Echelon et dont l'activité est décrite dans le rapport STOA sur le développement des technologies de surveillance et le risque d'abus d'informations économiques;

- vérifier la compatibilité d'un tel système avec le droit communautaire, en particulier l'article 286 du traité CE et les directives 95/46/CE et 97/66/CE, et avec l'article 6, paragraphe 2, du traité sur l'Union européenne, sur la base des questions suivantes:

- les droits des citoyens européens sont-ils protégés contre les activités des services secrets?

- le cryptage constitue-t-il une protection adéquate et suffisante pour protéger la vie privée des citoyens ou faut-il prendre des mesures complémentaires et, dans l'affirmative, de quel ordre?

- comment renforcer la prise de conscience des institutions européennes à l'égard des risques suscités par ces activités, et quelles mesures peut-on prendre?

- vérifier si l'interception des communications au niveau mondial fait courir des risques à l'industrie européenne,

- proposer, le cas échéant, des initiatives politiques et législatives."

---

[6] Raytheon Corp Press release, http://raytheon.com/sivam/contract.html; *Scott Shane, Tom Bowman*, America's Fortress of Spies, Baltimore Sun, 3.12.1995.

[7] Résolution du Parlement européen du 5 juillet 2000, B-5 – 0593/2000, JO C 121/131 du 24.4.2001.

1.4. Pourquoi n'avoir pas opté pour une commission d'enquête?

Si le Parlement européen opta donc pour la constitution d'une commission temporaire, c'est que la constitution d'une commission d'enquête n'est possible qu'aux fins d'examiner des violations du droit communautaire dans le cadre du traité CE (article 193 TCE) et que dès lors, une commission d'enquête ne peut se saisir que des matières qui y sont visées. Les domaines qui ressortissent au titre V (PESC) et au titre VI TUE (Coopération policière et judiciaire en matière pénale) sont exclus. De plus, selon la décision interinstitutionnelle[8], une commission d'enquête ne peut exercer les droits spécifiques qui sont les siens en matière d'audition et de consultation des dossiers que dans le cas où des motifs de secret ou de sécurité publique ou nationale ne s'y opposent pas, ce qui empêche d'inviter des membres des services secrets à comparaître. De même, une commission d'enquête ne peut étendre ses travaux à des pays tiers, dès lors que, par définition, ceux-ci ne peuvent violer le droit de l'Union européenne. Comme la constitution d'une commission d'enquête aurait impliqué des limites quant au travail de fond, sans donner des droits supplémentaires, la majorité des députés au Parlement européen a rejeté cette solution.

1.5. Méthode et plan de travail

Pour pouvoir exercer pleinement et entièrement son mandat, la commission a opté pour la procédure suivante. Un programme de travail, proposé par votre rapporteur et adopté par la commission, dressait une liste des grands thèmes concernés:

1. connaissances sûres relatives à ECHELON,
2. discussion dans les parlements et gouvernements nationaux,
3. services de renseignement et activités de ceux-ci,
4. systèmes de communication et possibilité de les intercepter,
5. cryptage,
6. espionnage économique,
7. objectifs de l'espionnage et mesures de protection, et
8. cadre juridique et protection de la sphère privée,
9. conséquences sous l'angle des relations extérieures de l'UE.

Ces thèmes ont ensuite été étudiés au cours de différentes réunions, l'ordre de leur examen étant dicté par des points de vue pratiques et non par la plus ou moins grande importance attachée à chacun d'eux. Pour préparer chacune des réunions, votre rapporteur a consulté et exploité de façon systématique la documentation existante. Compte tenu des nécessités liées à l'examen du point concerné, furent invités aux différentes réunions des représentants des administrations nationales (et notamment des services secrets) ainsi que des parlements nationaux, qui sont les organes de contrôle des services secrets, tout comme des experts juridiques et des experts dans les domaines des techniques de communication et d'interception, de la sécurité des entreprises et des techniques de cryptage, experts appartenant tant au monde scientifique qu'au monde des affaires. Des journalistes qui avaient effectué des travaux de recherche sur ce thème furent également invités. En règle générale, les réunions étaient publiques, ce qui n'empêche que le huis clos a également été décidé, quand il pouvait être utile pour obtenir des informations. De plus, le

[8] Décision du Parlement européen, du Conseil et de la Commission, du 19 avril 1995, portant modalités d'exercice du droit d'enquête du Parlement européen (95/167/CE, Euratom, CECA), art. 3, paragraphes 3, 4 et 5.

président de la commission et votre rapporteur se sont rendus, ensemble, à Londres et à Paris, pour y rencontrer des personnes, qui, pour différentes raisons, ne pouvaient pas participer aux réunions de la commission, mais qu'il semblait toutefois utile d'associer aux travaux de celle-ci. Pour les mêmes raisons, le bureau de la Commission, les coordinateurs et votre rapporteur se sont rendus aux États-Unis. Par ailleurs, votre rapporteur a également eu de nombreux entretiens individuels, parfois confidentiels.

1.6. Caractéristiques attribuées au système ECHELON

Le système désigné sous le nom de code "ECHELON", se distingue des autres systèmes de renseignement par le fait qu'il présente deux caractéristiques lui conférant un niveau de qualité tout particulier.

La première qu'il est réputé avoir, c'est la capacité d'exercer une surveillance pour ainsi dire totale. Par l'intermédiaire surtout de stations de réception satellitaire et de satellites–espions, toute communication d'une personne transportée sur n'importe quel support – téléphone, téléscripteur, réseau Internet ou courrier électronique – peut être interceptée aux fins de prendre connaissance de son contenu.

La deuxième, c'est que le système "ECHELON" exerce ses activités à l'échelle planétaire grâce à la coopération de plusieurs États (Royaume-Uni, États-Unis, Canada, Australie et Nouvelle-Zélande), ce qui constitue un plus par rapport aux systèmes nationaux: les pays parties au système ECHELON (pays UKUSA)[9] peuvent se partager l'utilisation de leurs installations d'interception, les tâches en résultant et les renseignements obtenus. Cette coopération internationale est justement essentielle pour la surveillance à l'échelle mondiale des communications par satellite, car elle seule permet, dans les communications internationales, d'intercepter les deux parties d'une conversation. Il est parfaitement évident que compte tenu de leurs dimensions, des stations de réception satellitaire ne peuvent être construites sur le territoire d'un pays sans son assentiment. L'accord réciproque et la coopération – dans une mesure plus ou moins grande – de plusieurs pays situés en différents points du monde est en l'occurrence indispensable.

[9] V. chapitre 5, point 5.4.

Les risques que pourrait présenter, pour la sphère privée et les milieux économiques, un système du type ECHELON ne résultent pas uniquement du très grand potentiel de ce système de surveillance, mais procèdent bien davantage du fait qu'il fonctionne dans un espace qui échappe, pour l'essentiel, à toute règle juridique. Un système d'interception des communications internationales ne vise pas la plupart du temps les habitants du pays qui l'exploite. De par son statut d'étranger, la personne dont les messages sont interceptés ne dispose ainsi d'aucune protection juridique intérieure. Aussi, l'individu est-il entièrement à la merci du système. Dans ce domaine, le contrôle parlementaire est également insuffisant, dès lors que les électeurs, qui partent du principe qu'ils ne sont pas concernés et que "seules" sont concernées des personnes à l'étranger, ne manifestent pas un intérêt particulier pour cette question, et que pour les élus, ce qui compte avant tout, ce sont les intérêts de leurs électeurs. Aussi ne faut-il pas s'étonner que les auditions sur les activités de la NSA, qui ont eu lieu au sein du Congrès américain, aient porté uniquement sur la question de savoir si des citoyens américains étaient également victimes de ce système, dont l'existence même n'a pas suscité de véritables réserves. Il est dès lors d'autant plus nécessaire d'engager un débat en la matière à l'échelle européenne.

2. Activité des services de renseignements extérieurs

2.1. Introduction

Pour garantir la sécurité de l'État, la plupart des gouvernements font appel non seulement à la police mais aussi aux services de renseignement. Ceux-ci, dès lors que leur activité est, la plupart du temps, secrète, sont également appelés services secrets. Ces services ont pour mission:

– de recueillir des informations permettant de parer à tout danger pour la sécurité de l'État,
– de se livrer, en règle générale, au contre-espionnage,
– de parer aux risques susceptibles de menacer les forces armées, et
– de recueillir des informations sur des développements à l'étranger.

2.2. Que faut-il entendre par espionnage?

Pour les gouvernements, il est essentiel de recueillir et d'exploiter de façon systématique des informations sur certains développements dans d'autres pays. Ce qu'ils recherchent en l'occurrence, ce sont des bases pour des décisions à prendre dans le domaine des forces armées, de la politique étrangère, etc. Aussi se sont-ils dotés de services de renseignement extérieur. Dans un premier temps, ces services s'emploient à exploiter systématiquement des sources d'information librement accessibles. D'après ce qui lui a été dit, votre rapporteur considère que cette activité représente en moyenne au moins 80 % de l'activité des services de renseignement[10]. Il n'empêche que des informations particulièrement importantes dans ces domaines sont tenues secrètes par les gouvernements ou les entreprises, et que chacun n'y a donc pas accès. Celui qui veut pourtant se les approprier, il doit les voler. L'espionnage n'est rien d'autre que le vol organisé d'informations.

2.3. Objectifs de l'espionnage

Les objectifs classiques de l'espionnage sont les secrets militaires, les secrets d'autres gouvernements ou des informations concernant la stabilité des gouvernements ou les risques auxquels ils sont exposés. Sont visés, par exemple, les nouveaux systèmes d'armement, les stratégies militaires, ou des informations concernant le stationnement des troupes. Non moins importantes sont les informations relatives à des décisions imminentes en matière de politique étrangère, les décisions monétaires ou les informations d'initiés concernant des tensions au sein d'un gouvernement. Parallèlement, un intérêt est également manifesté pour des informations importantes du point de vue économique, qui peuvent être non seulement des informations sectorielles mais aussi des renseignements précis sur de nouvelles technologies ou des contrats avec l'étranger.

[10] Dans son rapport "Preparing for the 21st Century: An Appraisal of U.S. Intelligence", la "Commission on the Roles and Capabilities of the US Intelligence Community" (1996) constate que 95 % de tous les renseignements d'ordre économique proviennent de sources publiques (chapitre 2 "The Role of intelligence"). http://www.gpo.gov/int/report.html

2.4. Méthodes de l'espionnage

L'espionnage signifie se procurer un accès à des informations que leur propriétaire souhaite justement préserver de la curiosité des tiers. Aussi faut-il venir à bout de cette protection et la jeter bas. Il en va exactement ainsi pour l'espionnage politique comme pour l'espionnage économique. C'est pourquoi l'espionnage dans ces deux secteurs pose les mêmes problèmes et les mêmes techniques d'espionnage sont mises en œuvre. Du point de vue logique, il n'y a pas de différence, hormis le niveau de protection, qui est dans le monde économique la plupart du temps moindre, ce qui explique que l'espionnage économique se révèle souvent plus simple. La conscience du risque auquel expose l'utilisation de communications pouvant être interceptées est notamment moins nette dans le milieu économique que celle de l'État dans les domaines ressortissant à la sécurité.

2.4.1. Recours à l'être humain dans l'espionnage

La protection des informations secrètes se conçoit toujours de la même façon:

- le nombre de personnes, jugées sûres, ayant accès aux informations secrètes est limité;
- des prescriptions strictes régissent l'usage de ces informations;
- normalement, les informations ne sortent pas du secteur protégé, et si elles le font toutefois, c'est uniquement de façon sûre ou en étant codées. Aussi l'espionnage organisé s'attache-t-il tout d'abord à obtenir, par l'intermédiaire de **personnes** (ce qu'il est convenu d'appeler le renseignement humain), un accès direct et sans détour aux informations souhaitées. Il peut s'agir en l'occurrence:
    - de membres infiltrés (agents) du service/de l'entreprise, ou
    - de personnes recrutées au sein de la cible.

Ces dernières personnes travaillent pour des services/entreprises étrangers la plupart du temps pour les raisons suivantes:
- sexualité,
- corruption par l'argent ou par des positions lucratives,
- chantage,
- convictions idéologiques,
- conquête d'un statut ou d'un honneur particulier (appel au mécontentement ou sentiment d'infériorité).

Il existe un cas limite, celui de la coopération involontaire par "écumage". En l'occurrence, des collaborateurs d'autorités ou d'entreprises sont incités, en flattant leur vanité, et ce dans des conditions apparemment innocentes (conversations en marge de conférences, à l'occasion de congrès spécialisés, au bar d'un hôtel), à bavarder.

L'utilisation de personnes présente l'avantage d'offrir un accès direct aux informations souhaitées. Cette solution ne va toutefois pas sans inconvénients:

- l'attention du contre-espionnage se porte toujours sur les personnes ou les agents dirigeants;
- dans le cas de personnes recrutées, les points faibles qui ont incité à les recruter peuvent avoir un effet de boomerang;

- les personnes peuvent toujours commettre des erreurs et se retrouver donc, à un moment ou l'autre, prises dans les mailles du contre-espionnage.

Dès lors, on s'efforce, là où c'est possible, de substituer à l'utilisation d'agents ou de personnes recrutées un espionnage anonyme et non personnel. La solution la plus simple consiste à exploiter les signaux hertziens d'installations ou de véhicules possédant une importance au point de vue militaire.

2.4.2. Exploitation des signaux électromagnétiques

Pour l'opinion publique, la forme la plus connue de l'espionnage par des moyens techniques, c'est l'utilisation de la photographie par satellite. Néanmoins, il existe parallèlement une interception et une exploitation des signaux électromagnétiques, quelle qu'en soit la nature (SIGINT, ou mesure de renseignement électronique).

2.4.2.1. Signaux électromagnétiques ne servant pas aux communications

Certains signaux électromagnétiques, par exemple, les rayonnements produits par les stations radar, peuvent, dans le domaine militaire, fournir des informations précieuses sur l'organisation de la défense aérienne d'un opposant (ELINT, ou mesure de recherche électronique). De plus, les rayonnements électromagnétiques qui fournissent des indications sur la position des troupes, des avions, des bateaux ou des sous-marins, constituent une source d'information très utile pour un service de renseignement. De même, l'observation des satellites-espions d'autres pays, qui prennent des photos, et l'enregistrement ainsi que le décodage des signaux de ces satellites ne sont pas sans intérêt.

Les signaux sont captés par des stations fixes, des satellites sur orbite basse ou des satellites SIGINT quasi géostationnaires. Cette partie de l'activité des services secrets touchant aux signaux électromagnétiques absorbe, quantitativement, une partie importante des capacités d'interception des services, les possibilités techniques n'étant cependant pas pour autant épuisées.

2.4.2.2. Exploitation des communications interceptées

Les services de renseignement extérieur de nombreux pays interceptent les communications militaires et diplomatiques d'autres pays. Bien de ces services surveillent également, dans la mesure où ils y ont accès, les communications civiles d'autres pays. Dans certains pays, les services ont le droit de surveiller également les communications qui pénètrent sur le territoire national ou qui en sortent. Dans les démocraties, la surveillance des communications du **ressortissant national** par les services de renseignement est subordonnée à certaines conditions d'intervention et à certains contrôles. Les juridictions nationales ne protègent toutefois généralement que le citoyen et les autres personnes qui se trouvent sur son propre territoire. (cf. chapitre 8).

2.5. Activité de certains services de renseignements

C'est surtout l'activité d'interception des services de renseignement américain et britannique qui a déclenché le débat public. Les critiques visent l'ouverture et l'exploitation des communications (téléphonie vocale, téléscripteur, courrier électronique). Pour pouvoir émettre un jugement

politique, il faut une aune permettant de juger cette activité. Un critère de comparaison peut être l'activité d'interception des services de renseignement extérieurs dans l'Union européenne. Le tableau 1 ci-après expose de façon succincte la situation. Il démontre que l'interception des communications privées par les services de renseignement extérieur n'est pas propre aux seuls services américain et britannique.

Pays	Communications extérieures	Communication publiques	Communications privées
Belgique	+	+	-
Danemark	+	+	+
Finlande	+	+	+
France	+	+	+
Allemagne	+	+	+
Grèce	+	+	-
Irlande	-	-	-
Italie	+	+	+
Luxembourg	-	-	-
Pays-Bas	+	+	+
Autriche	+	+	-
Portugal	+	+	-
Suède	+	+	+
Espagne	+	+	+
Royaume-Uni	+	+	+
États-Unis	+	+	+
Canada	+	+	+
Australie	+	+	+
Nouvelle-Zélande	+	+	+

Tableau 1: Activités d'interception des services de renseignement dans l'Union européenne et dans les pays UKUSA

Signification des différentes colonnes:

1re colonne: pays concerné
2e colonne: communications extérieures, c'est-à-dire communications en provenance et à destination de l'étranger (civiles, militaires, diplomatiques)[11]
3e colonne: communications publiques (militaires, diplomatiques, etc.)
4e colonne: communications privées
\+ : interception
\- : pas d'interception

[11] Si le service de renseignement a accès au câble, il peut intercepter à la fois les communications provenant de l'étranger et les communications destinées à l'étranger. S'il a accès aux communications pas satellite, celui-ci se limite au *downlink*, mais l'ensemble des communications transportées peuvent être interceptées, y compris donc celles qui ne sont pas destinées à son territoire. Étant donné que la couverture des satellites s'étend généralement à l'ensemble de l'Europe ou à des régions plus vastes encore (voir 4.4.2.5.), une station de réception de satellite permet d'intercepter les communications par satellite de toute l'Europe dans un pays européen.

3. Conditions techniques minimales requises pour l'interception des télécommunications

3.1. Possibilité d'interception des différents supports des télécommunications

Lorsque deux personnes se trouvant à une certaine distance l'une de l'autre souhaitent communiquer entre elles, elles ont besoin d'un support de communication, qui peut être:

– l'air (son),
– la lumière (clignotant morse, câble à fibres optiques),
– l'électricité (télégraphe, téléphone),
– une onde électromagnétique (la radio sous ses formes différentes).

Le tiers qui s'assure un accès au support de la communication peut intercepter celle-ci. L'accès peut être aisé ou compliqué, possible de partout ou uniquement à partir de certaines positions. Ci-après, deux cas extrêmes sont examinés: les possibilités techniques pour un espion sur place, d'une part, et les possibilités pour un système d'interception fonctionnant à l'échelle mondiale, d'autre part.

3.2. Possibilités d'interception sur place[12]

Sur place, toute communication peut être interceptée, pour autant que l'espion soit résolu à commettre une infraction et que la victime de l'interception ne se protège pas.

– Dans des locaux, les **conversations** peuvent être interceptées en dissimulant des microphones (des mouchards) ou en analysant au moyen d'un laser les vibrations d'une fenêtre.

– Les **écrans** émettent des rayons qui peuvent être captés jusqu'à une distance de 30 m; ce qui apparaît sur l'écran est ainsi visible.

– Les **téléphones, téléscripteurs et courriers électroniques** peuvent être interceptés, si l'espion se branche sur le câble sortant du bâtiment.

– Un **téléphone portable** peut être intercepté – moyennant un gros effort technique – si la station d'interception se situe dans la même cellule (rayon: 150 m en ville, 15 km à la campagne).

– Un **émetteur de radio interne** peut être intercepté dans la limite des ondes radio ultracourtes.

[12] *Manfred Fink*, Lauschziel Wirtschaft – Abhörgefahren und –techniken, Vorbeugung und Abwehr, Richard Boorberg Verlag, 1996.

Sur place, les conditions d'utilisation des moyens techniques d'espionnage sont idéales, dès lors que les mesures d'interception peuvent être limitées à une seule personne cible ou à un seul objet cible, et qu'il est possible de capter pratiquement toute communication. Le seul inconvénient, c'est un certain risque de découverte, qui n'existe cependant que dans le cas du placement de "mouchards" ou du branchement sur le câble sortant du bâtiment.

3.3. Possibilités d'un système d'interception fonctionnant à l'échelle mondiale

Aujourd'hui, il existe, pour les communications intercontinentales, différents supports pour tous les types de communications (voix, fax et données). Les possibilités d'un système d'interception fonctionnant à l'échelle mondiale sont limitées par deux facteurs:

– l'accès limité au support de la communication,
– la nécessité de filtrer les communications intéressantes dans une masse gigantesque de communications effectuées.

3.3.1. Accès aux supports des télécommunications

3.3.1.1. Communications tributaires du câble

Le câble sert à acheminer toutes sortes de communications (voix, fax, courrier électronique, données). Les communications tributaires du câble ne peuvent être interceptées que dans le cas où un accès au câble est possible. Dans tous les cas, un accès est possible au point d'arrivée d'une liaison par câble, si celui-ci se situe sur le territoire de l'État qui fait procéder à l'interception. À l'intérieur des frontières d'un pays, toutes les communications par câble peuvent donc, **technique parlant**, être interceptées, à partir du moment où l'interception est autorisée par la justice. Les services de renseignement n'ont toutefois pas, la plupart du temps, un accès légal, aux câbles sur le territoire d'autres pays. Bien entendu, ils peuvent s'assurer, de façon tout à fait illégale, un accès ponctuel, en s'exposant à un grand risque de découverte.

À l'époque du télégraphe, les liaisons intercontinentales par câble avaient pour support des câbles sous-marins. Un accès à ces câbles est toujours possible là où ils ressortent de l'eau. Si plusieurs États exploitent en commun un réseau d'interception, alors, un accès est possible à toutes les extrémités des câbles sur le territoire de ces États. Historiquement, cela n'a pas été sans importance, les câbles télégraphiques sous-marins et les premiers câbles téléphoniques coaxiaux sous-marins entre l'Europe et l'Amérique ressortant de la mer à Terre-Neuve (Canada) et les liaisons avec l'Asie s'effectuant via l'Australie, des amplificateurs intermédiaires étant nécessaires. Aujourd'hui, les câbles à fibres optiques – qui peuvent être posés quel que soit le relief sous-marin – se voient équiper des amplificateurs intermédiaires nécessaires, ce qui permet un acheminement direct, c'est-à-dire sans relais en Australie ou en Nouvelle-Zélande.

S'agissant des câbles électriques, il est également possible de faire, entre les extrémités d'une liaison, un branchement par induction (c'est-à-dire par un procédé électromagnétique dans lequel une bobine est disposée sur le câble), sans réaliser une liaison électroconductrice directe. Cette technique peut également mise en œuvre, non sans lourdes dépenses, au départ des sous-marins, dans le cas de câbles électriques sous-marins. Les États-Unis y ont eu recours pour se brancher sur un certain câble sous-marin soviétique, par lequel des ordres non codés étaient transmis aux

sous-marins atomiques. Une telle technique ne saurait être généralisée, ne serait-ce qu'en raison de son coût.

Dans le cas des câbles à fibres optiques de l'ancienne génération actuellement utilisés, un branchement par induction n'est possible qu'au niveau des amplificateurs intermédiaires. Ceux-ci transforment le signal optique en un signal électrique, l'amplifient et le retransforment ensuite en un signal optique. Se pose toutefois la question de savoir comment la quantité gigantesque de données qui est transportée par un tel câble pourrait bien être acheminée entre le lieu de son interception et celui de son exploitation sans mettre en place un autre câble à fibres optiques. L'utilisation d'un sous-marin équipé des dispositifs techniques d'exploitation ne peut être envisagée, en raison des dépenses, que dans des cas extrêmement rares. Par exemple, en cas de guerre, le but étant d'intercepter les communications militaires et stratégiques de l'ennemi. S'agissant de la surveillance quotidienne des télécommunications internationales, l'utilisation d'un sous-marin est, de l'avis de votre rapporteur, exclue. Dans les câbles à fibres optiques de la dernière génération, l'amplificateur intermédiaire est un laser à l'erbium, et ce type d'amplificateurs ne permet plus un branchement électromagnétique aux fins de l'interception. Pour de tels câbles à fibres optiques, l'interception n'est possible qu'aux extrémités de la liaison.

Dans la pratique, cela signifie, pour le réseau d'interception des **pays UKUSA**, que ces pays ne pourraient, sans s'exposer à des dépenses déraisonnables, procéder à des interceptions qu'aux extrémités des câbles sous-marins, se trouvant sur leur territoire. En résumé, ils ne peuvent intercepter que les communications tributaires du câble aboutissant chez eux ou partant de chez eux! Ce qui signifie qu'**en Europe**, l'accès à la communication par câble à l'entrée et à la sortie du territoire n'est possible que sur **le territoire du Royaume-Uni!** Car, jusqu'ici, les communications intérieures continuent, la plupart du temps, à être acheminées par le réseau câblé intérieur; la privatisation des télécommunications peut générer des exceptions, mais celles-ci sont partielles et non prévisibles!

Tel est à tout le moins le cas pour le téléphone et le téléscripteur. Pour les communications Internet via le câble, la situation est différente. Sans trop s'étendre, il est possible de formuler les observations de nature restrictive suivantes:

- dans le réseau Internet, les communications s'effectuent par paquets de données, des paquets adressés à un destinataire pouvant suivre différents itinéraires dans le réseau;

- au début Internet, des créneaux non saturés du réseau scientifique public furent utilisés pour la transmission du courrier électronique. Le cheminement d'un message était dès lors tout à fait imprévisible, chaque paquet suivant un itinéraire chaotique qui ne pouvait être deviné. À l'époque, la principale liaison internationale était la "dorsale scientifique" entre l'Europe et l'Amérique;

- la commercialisation Internet et l'apparition de fournisseurs Internet entraîna également une commercialisation du réseau. Les fournisseurs Internet exploitaient ou louaient leurs propres réseaux. Aussi s'efforcèrent-ils de plus en plus souvent de confiner les communications à l'intérieur du réseau leur appartenant, en sorte d'éviter de devoir payer des redevances d'utilisation à d'autres opérateurs du réseau. Dès lors, l'itinéraire d'un paquet de données dans le réseau est aujourd'hui déterminé non seulement par le degré de saturation du réseau, mais

aussi par des considérations financières;

- un courrier électronique qui est envoyé par un client d'un fournisseur à un client d'un autre fournisseur reste en règle générale dans le réseau de l'entreprise, même si l'itinéraire qu'il suit alors n'est pas le plus rapide. Les ordinateurs qui sont disposés aux nœuds du réseau et qui décident du transport des paquets de données (les "routeurs") effectuent le transfert vers d'autres réseaux à certains points de connexion (les "commutateurs");

- à l'époque de la dorsale scientifique, les "commutateurs" de la communication Internet mondiale étaient situés aux États-Unis. Aussi, les services de renseignement pouvaient-ils alors y mettre la main sur une partie essentielle des communications Internet européennes. Aujourd'hui, les communications Internet intraeuropéennes ne transitent plus que dans une mesure très limitée par les États-Unis[13];

- une petite partie des communications intraeuropéennes sont acheminées via un commutateur à Londres, auquel le GCHQ britannique (Centre national de communications) a accès – étant donné qu'il s'agit de communications avec l'étranger. La plus grande partie des communications ne sortent pas du continent. C'est ainsi, par exemple, que plus de 95 % des communications Internet allemandes sont traitées par un commutateur situé à Francfort.

Dans la pratique, cela signifie que les États UKUSA ne peuvent avoir accès qu'à une **partie très limitée** des communications Internet tributaires du câble.

3.3.1.2. Communications hertziennes[14]

La possibilité d'intercepter des communications hertziennes dépend de la portée des ondes électromagnétiques utilisées. Si les ondes radio émises suivent la courbe de la surface terrestre (les **ondes de sol**), leur portée est limitée et dépend de la nature du sol, des constructions et de la végétation. Si les ondes radio sont envoyées vers l'espace (les **ondes d'espace ou indirectes**), elles peuvent franchir des distances considérables après réflexion sur les couches de l'ionosphère. Des réflexions successives augmentent notablement la portée.

La portée dépend de la longueur d'onde:

- les ondes myriamétriques et les ondes longues (3 kHz – 300 kHz) ne se propagent que via l'onde de sol, dès lors que l'onde d'espace n'est pas reflétée. Leur portée est limitée;

- les ondes moyennes (300 kHz – 3MHz) se propagent via l'onde de sol et, la nuit, également via l'onde d'espace. Elles ont une portée moyenne;

---

[13] Une version de démonstration de *Visual Route*, programme qui indique le chemin suivi par une communication Internet, a permis de montrer qu'une communication avec le Royaume-Uni, la Finlande ou la Grèce à partir de l'Allemagne passe par les États-Unis et le Royaume-Uni. De même pour une communication d'Allemagne vers la France. À partir du Luxembourg, la communication vers la Belgique, la Grèce, la Suède ou le Portugal passe par les États-Unis, les communications à destination de l'Allemagne, de la Finlande, de la France, de l'Italie, des Pays-Bas ou de l'Autriche par le *switch* londonien. http://visualroute.cgan.cpm.hk/

[14] U. Freyer, Nachrichtenübertragungstechnik, Hanser Verlag, 2000.

- les ondes courtes (3MHz – 30 MHz) se propagent principalement via l'onde d'espace et permettent, par réflexions successives, une réception **circumterrestre;**

- les ondes ultracourtes (30 MHz – 300 MHz) se propagent uniquement via l'onde de sol, dès lors que l'onde d'espace n'est pas reflétée. Elles se propagent plutôt en ligne droite, comme la lumière, leur portée dépendant ainsi, compte tenu de la courbure de la terre, de la hauteur des antennes de l'émetteur et du récepteur. Selon la puissance, leur portée peut atteindre quelque 100 km (pour les téléphones portables, 30 km environ);

- les ondes décimétriques et centimétriques (30 MHz – 30 GHz) se propagent davantage encore que les ondes ultracourtes de façon quasi-optique. Elles peuvent facilement être réunies en faisceaux, ce qui permet des transmissions ciblées à faible puissance (faisceaux hertziens terrestres). Elles ne peuvent être captées que par une antenne très proche, parallèlement, du faisceau hertzien ou située dans l'axe de celui-ci ou dans son prolongement.

Les ondes longues et moyennes ne sont utilisées que pour les émetteurs radio, les radiophares, etc. Les communications radio militaires et civiles s'effectuent par ondes courtes, et surtout par ondes ultracourtes et ondes décimétriques/centimétriques.

Il ressort des observations qui précèdent qu'un système d'interception des communications fonctionnant à l'échelle mondiale ne peut avoir accès qu'aux émissions en ondes courtes. Pour tous les autres types d'émissions hertziennes, la station d'interception doit être située à 100 km ou moins (par exemple sur un bateau, dans une ambassade).

Dans la pratique, cela signifie que les pays UKUSA ne peuvent avoir accès, grâce aux stations d'interception terrestres, qu'à une partie très limitée des communications hertziennes.

3.3.1.3. Communications via des satellites de télécommunication géostationnaires[15]

Comme il a déjà été dit, les ondes décimétriques et centimétriques peuvent être facilement réunies en faisceaux hertziens. Si un faisceau hertzien est dirigé vers un satellite de communication stationnaire sur orbite haute, satellite qui reçoit, transforme et renvoie les signaux hertziens vers la terre, il est possible de franchir de grandes distances sans utiliser le câble. En réalité, la portée d'une telle liaison n'est limitée que par le fait que le satellite ne peut recevoir des signaux venant de toute la terre ni envoyer des signaux vers toute la terre. Aussi faut-il plusieurs satellites pour obtenir une couverture planétaire. (Pour plus de détails, se référer au chapitre 4.) Si les pays UKUSA ont mis en place des stations d'interception dans les régions requises de la terre, ils peuvent en principe intercepter l'ensemble des communications – téléphone, fax et données – effectuées via de tels satellites.

[15] Hans Dodel, Satellitenkommunikation, Hüthig Verlag, 1999.

3.3.1.4. Possibilités d'interception par avion et bateau

L'on sait, depuis longtemps, que des avions spéciaux du type AWACS sont utilisés pour repérer dans le monde entier d'autres avions. Le radar de ces appareils est complété par un système d'identification d'objectifs donnés, qui peut repérer des rayonnements électroniques, les classifier et les corréler avec des contacts radar. Il n'existe pas une capacité SIGINT distincte[16]. En revanche, l'avion-espion EP-3 des forces navales américaines, qui vole à faible vitesse, dispose de possibilités d'interception dans la bande des micro-ondes, des ondes ultracourtes et des ondes courtes. Les signaux sont exploités directement à bord; l'appareil sert uniquement à des fins militaires[17].

De plus, des navires de surface et, à proximité des terres des sous-marins sont utilisés pour intercepter les communications radio militaires[18].

3.3.1.5. Possibilités d'interception par satellite-espion

Lorsqu'elles ne sont pas réunies en faisceau par des antennes appropriées, les ondes radio se propagent dans toutes les directions, y compris vers l'espace. Les satellites SIGINT sur orbite basse ne peuvent garder le contact avec l'émetteur recherché que pendant quelques minutes. Dans les zones fortement peuplées et très industrialisées, l'interception est rendue plus difficile par la densité importante d'émetteurs de même fréquence, à un tel point qu'il n'est pratiquement pas possible de filtrer les signaux[19]. Ces satellites ne se prêtent pas à une surveillance en continu des communications radio civiles.

Parallèlement, il existe des satellites SIGINT américains dits quasi-stationnaires sur orbite haute (42 000 km)[20]. Contrairement aux satellites de communication géostationnaires, ces satellites présentent une inclinaison de 3 à 10°, un apogée de 39 000 à 42 000 km et un périgée de 30 000 à 33 000 km Les satellites ne sont donc pas immobiles sur leur orbite; ils se déplacent selon une orbite elliptique complexe. Aussi peuvent-ils, au cours d'une journée, couvrir une région plus grande et permettent-ils de repérer des sources radio. Il semble bien dès lors, et compte tenu également des autres caractéristiques du domaine public, que l'utilisation de ces satellites est purement militaire.

Les signaux reçus sont retransmis vers une station terrestre par une puissante liaison descendante en faisceaux de 24 GHz.

3.3.2. Possibilités d'exploitation automatique des communications interceptées: utilisation de filtres

Lorsque les communications extérieures sont l'objet de l'interception, celle-ci ne vise pas un raccordement téléphonique donné. Le but consiste plutôt à intercepter l'ensemble ou une partie des communications effectuées via les satellites surveillés ou le câble surveillé et à les filtrer au moyen d'ordinateurs en utilisation des notions clés. Et cela parce que l'exploitation de l'ensemble

[16] Lettre de Walter Kolbow, Secrétaire d'État au ministère fédéral de la défense au rapporteur, en date du 14.2.2001.
[17] Süddeutsche Zeitung, n° 80 du 5.4.2001, 6.
[18] *Jeffrey T. Richelson*, The U.S. Intelligence Community, Ballinger, 1989, 188 et 190.
[19] Lettre de Walter Kolbow, Secrétaire d'État au ministère fédéral de la défense, en date du 14.2.2001.
[20] Major *A. Andronov*, Zarubezhnoye voyennoye obozreniye, n° 12, 1993, 37 à 43.

des communications interceptées est tout à fait impossible.

Le filtrage des communications effectuées par des raccordements donnés est simple. En utilisant des notions clés, il est également possible de saisir de façon spécifique les téléfax et les courriers électroniques. Il est même possible de repérer une voix donnée, si le système a été formé pour reconnaître celle-ci[21]. Par contre, la reconnaissance automatique de mots prononcés par une voix quelconque n'est, selon les informations en possession de votre rapporteur, pas possible actuellement avec une précision suffisante. De plus les possibilités de filtrage sont encore limitées par d'autres facteurs: la capacité finale de l'ordinateur, le problème des langues et, surtout, le nombre limité des experts capables de lire et d'exploiter les informations filtrées. Dans le contexte de l'appréciation des possibilités des systèmes de filtrage, il faut également tenir compte du fait que l'ensemble des possibilités techniques d'un tel système d'interception fonctionnant selon le "principe de l'aspirateur" sont ventilées selon différents thèmes. Une partie des mots clés concerne la sécurité militaire, une deuxième le trafic de drogue et d'autres formes de criminalité internationale, une troisième des notions relatives au commerce des biens à double usage et une quatrième le respect d'embargos. Une autre partie des notions clés a également trait à l'économie. Il en résulte que les capacités du système s'éparpillent entre plusieurs secteurs. Une concentration des mots clés sur le seul secteur intéressant du point de vue économique serait contraire aux priorités que les dirigeants politiques imposent à ces services; une telle réorientation n'a jamais eu lieu, même après la fin de la guerre froide[22].

3.3.3. Exemple du service de renseignements allemand

La deuxième section du service fédéral de renseignement allemand (BND) se procure des informations par l'interception des communications étrangères. Cette activité a fait l'objet d'un examen par la Cour constitutionnelle allemande. Les détails qui ont été rendus publics à cette occasion[23] donnent – conjointement avec les déclarations faites par le coordinateur des services secrets au sein de la chancellerie fédérale, Ernst Uhrlau, devant la commission ECHELON, le 21 novembre 2000 – une idée des possibilités des services de renseignement en matière d'interception des communications par satellite (jusqu'au mois de mai 2001, l'interception de communications par câble avec l'étranger n'était pas autorisée en Allemagne).

Il se peut que, çà et là, d'autres services de renseignement aient davantage de possibilités importantes, dans la mesure où l'accès aux communications tributaires du câble leur est permis ou si plus de personnes se consacrent à l'exploitation des informations. Si les communications tributaires du câble sont également interceptées, la probabilité statistique de réussite est notablement augmentée, ce qui n'est pas le cas nécessairement du nombre de communications exploitables. En fait, le cas du BND constitue, pour votre rapporteur, un exemple frappant des possibilités et stratégies des services de renseignement étrangers dans le domaine de l'interception des communications extérieures, même s'ils n'en font pas publiquement état.

Par la voie d'un contrôle **stratégique** des télécommunications, le service de renseignement fédéral s'efforce d'obtenir à l'étranger des informations concernant l'étranger. À cet effet, les communications satellitaires sont interceptées en se fondant sur une série de notions cibles (qui,

[21] Communication faite en privé au rapporteur, source protégée.
[22] Communication faite en privé au rapporteur, source protégée.
[23] BVerfG, 1 BvR 2226/94 du 14.7.1999, paragraphe 1.

en Allemagne, doivent être autorisées préalablement par la commission G10[24]). Quantitativement, le schéma se présente comme suit (état 2000): sur les quelque 10 millions de communications internationales/jour effectuées au départ et à destination de l'Allemagne, 800 000 environ le sont par satellite. À peine 10% d'entre elles (75 000) sont filtrées par un appareil de recherche. Cette situation s'explique, de l'avis de votre rapporteur, non par des raisons légales (en théorie, la totalité aurait été permise, à tout le moins avant le procès devant la Cour constitutionnelle), mais bien par des raisons techniques dues à certaines contraintes, comme la capacité d'exploitation.

De même, le nombre des notions de recherche pouvant être utilisées est limité tant par la technique que par l'autorisation préalable requise. Dans la motivation de son arrêt, la Cour constitutionnelle fait état, parallèlement aux notions de recherche purement formelles (interception d'étrangers ou d'entreprises étrangères à l'étranger), de 2 000 notions de recherche dans le domaine de la prolifération, de 1 000 dans le domaine du commerce des armes, de 500 dans le domaine du terrorisme et de 400 dans le domaine du trafic de drogue. S'agissant du terrorisme et du trafic de drogue, la procédure ne semble toutefois pas avoir été une réussite particulière.

L'appareil de recherche étudie les notions de recherche autorisées transmises par téléfax et par télex. Une reconnaissance automatique de mots n'est actuellement pas possible dans les communications vocales. Si les notions de recherche ne sont pas découvertes, les communications finissent automatiquement, de par la technique appliquée, dans la poubelle; elles ne peuvent pas être exploitées, parce qu'il n'existe aucune base juridique le permettant. Quotidiennement, quelque 5 communications d'utilisateurs des télécommunications relèvent de la protection de la constitution allemande. L'interception stratégique du service fédéral de renseignement vise à trouver des éléments pouvant servir de base pour une autre interception. Son objectif ne consiste pas à instaurer une surveillance absolue des communications extérieures. Selon les informations dont il dispose, votre rapporteur estime qu'il en est également ainsi pour l'activité SIGINT d'autres services de renseignement étranger.

[24] Gesetz zur Beschränkung des Brief-,Post- und Fernmeldegeheimnisses (Gesetz zu Artikel 10 GG) du 13.8.1968.

4. Technique des communications satellitaires

4.1. Importance des satellites de télécommunication

Les satellites de communication forment aujourd'hui un élément indispensable du réseau mondial des télécommunications et de la diffusion de programmes de radio et de télévision, ainsi que de services multimédias. Néanmoins, la part des communications par satellite dans les communications internationales a fortement diminué ces dernières années en Europe centrale. Elle se situe entre 0,4 et 5 %[25]. Cette situation s'explique par les avantages que présente le câble à fibres optiques, qui peut acheminer un nombre bien plus important de communications, tout en garantissant une qualité élevée.

Désormais, les communications sont numérisées y compris dans le secteur vocal. La capacité des liaisons satellitaires numériques par transpondeur de satellite est limitée à **1890** canaux vocaux RNIS (64 kbits/sec). En revanche, une seule fibre optique peut aujourd'hui déjà offrir **241920** canaux vocaux à la même norme. Le rapport est ainsi de **1 à 128**!

De plus, la qualité des liaisons par satellite est moindre que celle des liaisons par câble marin à fibres optiques. Les pertes de qualité dues à la longueur du temps de parcours des signaux – plusieurs centaines de millisecondes – sont à peine perceptibles dans une transmission vocale normale, ce qui n'empêche qu'il est possible de percevoir le décalage. Pour les communications de données et de téléfax, qui s'effectuent par l'intermédiaire d'une procédure complexe de mise en liaison, le câble présente des avantages évidents en termes de sécurité de liaison. Force est toutefois de constater, parallèlement, que 15% de la population mondiale seulement est connectée au réseau mondial de câbles[26].

Aussi, les systèmes satellitaires demeureront-ils cependant plus avantageux que le câble pour certaines applications. Citons quelques exemples civils:

- acheminement national, régional et international de communications téléphoniques et de données dans des régions où le volume des communications est restreint, c'est-à-dire là où la réalisation d'une liaison par câble ne serait pas rentable compte tenu du taux d'utilisation;

- communication limitée dans le temps pour des interventions en cas de catastrophes, des manifestations, des chantiers importants, etc.;

- missions des Nations unies dans des régions où les infrastructures de communication sont peu développées;

- communication économique flexible/mobile avec des petits émetteurs (VSAT, cf. infra).

Cette gamme d'utilisation des satellites dans les communications trouve son origine dans les caractéristiques suivantes: les émissions d'un seul satellite géostationnaire peuvent couvrir près de 50% de la surface terrestre; des terrains impraticables peuvent également être franchis. Ainsi, 100% des utilisateurs, qu'ils soient terrestres, marins ou aériens, peuvent être desservis. Les

[25] Indications fournies par les opérateurs de quelques États membres à la demande de la commission.
[26] Page d'accueil de Deutsche Telekom: www.detesat.com/deutsch/.

satellites sont opérationnels en quelques mois, et ce indépendamment de l'infrastructure locale. Ils sont plus sûrs que le câble et peuvent être mis hors service facilement.

Les caractéristiques suivantes des communications satellitaires appellent des commentaires négatifs: les temps de parcours relativement longs des signaux, la dégradation par éparpillement, la durée de vie – de 12 à 15 ans – plus courte que le câble, la plus grande vulnérabilité, ainsi que les possibilités plus importantes d'interception.

4.2. Fonctionnement d'une liaison satellitaire[27]

Comme il a été dit précédemment (cf. chapitre 3), les micro-ondes peuvent facilement être réunies en faisceaux. Il est dès lors possible de remplacer le câble par des faisceaux hertziens. Si les antennes d'émission et de réception ne se trouvent pas sur un même plan – ce qui est le cas sur terre, notre planète affectant la forme d'une sphère –, l'antenne de réception "disparaît" par suite de la courbure de la surface, à partir d'une certaine distance, sous l'horizon. Alors, les deux antennes ne se "voient" plus. Ce serait également le cas, par exemple, pour un faisceau hertzien intercontinental entre l'Europe et les États-Unis. Pour pouvoir établir une liaison, les antennes devraient se trouver au sommet de mâts hauts de 1,8 km Pour cette seule raison, un tel faisceau hertzien intercontinental ne peut être réalisé. D'autant plus que le signal est amorti par l'atmosphère et la vapeur d'eau sur l'ensemble du parcours. Toutefois, s'il est possible de disposer, à grande altitude, dans l'espace et sur une "position fixe", une sorte de miroir qui capte le faisceau hertzien, alors, de grandes distances peuvent être franchies en dépit de la courbure de la terre, la comparaison pouvant être faite avec un miroir routier qui permet de voir ce qu'il y a après un virage. Le principe décrit ci-dessus est mis en œuvre dans la pratique en utilisant des satellites dits géostationnaires.

4.2.1. Satellites géostationnaires

Si un satellite est placé sur orbite circulaire parallèle à l'équateur et fait un tour de la terre en 24 heures, alors il suit exactement la rotation terrestre. De la surface de la terre, il apparaît dès lors immobile à environ 36 000 km de distance. Il a une position **géostationnaire**. La plupart des satellites de télécommunications et de télévision appartiennent à ce type de satellites.

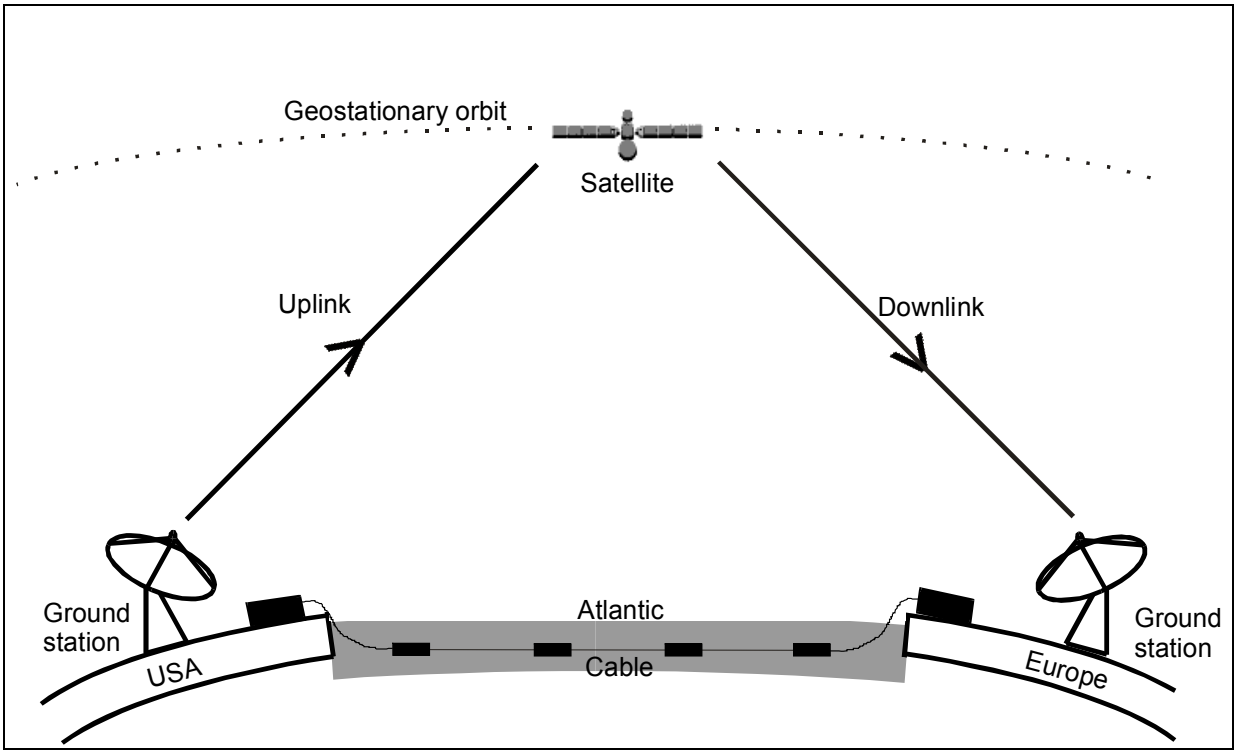
4.2.2. Cheminement d'une liaison satellitaire de télécommunication

La transmission des signaux via satellite s'effectue comme suit:

Le signal acheminé par une liaison est envoyé par une station terrestre équipée d'une antenne parabolique via un faisceau hertzien ascendant, appelé **uplink**, vers un satellite. Le satellite reçoit le signal, l'amplifie et le renvoie via un faisceau hertzien descendant, appelé **downlink**, vers une autre station terrestre. Là, le signal est réintroduit dans un réseau câblé.

[27] *Hans Dodel,* Satellitenkommunikation, Hüthig Verlag (1999), *Georg E. Thaller,* Satelliten im Erdorbit, Franzisverlag (1999).

Dans le cas de la communication mobile (par satellite), le signal est transmis directement de l'unité de communication mobile au satellite d'où il peut être réinjecté, via une station terrestre, dans un réseau ou directement retransmis à une autre unité mobile.



4.2.3. Principaux systèmes de communication satellitaires existants

Les communications provenant de **réseaux de câbles accessibles au public** (qui ne sont pas nécessairement publics) sont, le cas échéant, acheminées via des systèmes satellitaires de dimensions différentes entre des stations terrestres fixes, pour être ensuite réinjectées dans les réseaux de câbles. Une distinction est faite entre les systèmes satellitaires

- mondiaux (p. ex. INTELSAT),
- régionaux (continentaux) (p. ex. EUTELSAT), et
- nationaux (p. ex. ITALSAT).

La plupart de ces satellites se trouvent sur orbite géostationnaire. Dans le monde, 120 sociétés privées exploitent quelque mille satellites placés sur de telles orbites[28].

Parallèlement, il existe, pour le grand Nord, des satellites sur orbite spéciale très excentrique (orbites russes Molnyia), qui sont visibles pour l'utilisateur du grand Nord pendant plus de la moitié de leur période orbitale. Deux satellites de ce genre permettent en principe ainsi une couverture régionale[29], qui ne peut être obtenue à partir d'une position géostationnaire au-dessus de l'équateur. S'agissant des satellites russes Molnyia, en service depuis 1974 pour les

[28] *Georg E. Thaller*, Satelliten im Erdorbit, Franzisverlag, 1999.
[29] Vgl. dazu *Hans Dodel,* Satellitenkommunikation, Hüthig Verlag (1999)

communications (prototype dès 1964), 3 satellites parcourent en 12 heures une orbite circum-terrestre, à 120° de distance, assurant ainsi la transmission continue des communications[30].

De plus, le réseau INMARSAT – conçu au départ pour une utilisation à des fins maritimes - qui couvre le monde entier représente un **système de communication mobile**, permettant d'établir des liaisons satellitaires partout dans le monde. Il fait également appel à des satellites géostationnaires.

Le système de communication par portables IRIDIUM fonctionnant grâce à plusieurs satellites sur orbites basses différées a été mis hors service récemment, pour des raisons économiques, son taux d'utilisation étant insuffisant.

En outre, il existe un marché en rapide développement pour les communications VSAT (terminal équipé d'une très petite antenne). Il s'agit en l'occurrence de microstations dont l'antenne à un diamètre compris entre 0,9 et 3,7 m, qui sont exploitées par des entreprises pour leurs propres besoins (par exemple, des vidéoconférences) ou par des fournisseurs de services mobiles pour une demande temporaire de liaison (par exemple, des réunions). En 1996, 200 000 microstations étaient exploitées dans le monde entier. Le groupe Volkswagen exploite 3 000 unités VSAT, Renault 4 000, General Motors 100 000, et le plus grand groupe pétrolier européen 12 000. Les communications se font en clair, à moins que le client ne les crypte lui-même[31].

4.2.3.1. Systèmes de satellites fonctionnant à l'échelle mondiale

Ces systèmes de satellites couvrent l'ensemble de la planète grâce au positionnement de plusieurs satellites dans les zones atlantique, indienne et pacifique.

INTELSAT[32]

INTELSAT (Organisation internationale des télécommunications par satellites), qui a été créée en 1964, est une autorité dont la structure organisationnelle est similaire à celle des Nations unies, et dont l'activité consiste à assurer des communications internationales. Les membres de cette organisation étaient les administrations nationales des postes publiques. À l'heure actuelle, 144 gouvernements sont membres d'INTELSAT. L'année 2001 verra la privatisation d'INTELSAT.

INTELSAT dispose d'une flotte de 20 satellites géostationnaires, qui mettent en contact plus de 200 pays et dont les services sont loués à ses membres, lesquels disposent de leurs propres stations au sol. Grâce à IBS (Service commercial d'INTELSAT), des tierces parties (p. ex., des sociétés de téléphone, de grandes entreprises, des groupes internationaux) peuvent également utiliser les satellites depuis 1984. INTELSAT propose des services planétaires dans différents domaines, comme les communications, la télévision, etc. Les télécommunications s'effectuent sur bandes C et Ku (cf. infra).

[30] Homepage der Federation of American Scientists http://www.geo-orbit.org
[31] *Hans Dodel*, déclaration faite en privé.
[32] Page d'accueil d'INTELSAT – http://www.intelsat.com.

Les satellites d'INTELSAT sont les principaux satellites utilisés pour les communications internationales. Ils assurent l'essentiel des communications internationales satellitaires.

Ces satellites couvrent les zones atlantique, indienne et pacifique (cf. tableau, chapitre 5, point 5.3).

Au-dessus de l'Atlantique, il y a dix satellites positionnés entre les 304°Est et 359°Est; au-dessus de l'océan Indien, six satellites entre les 62°Est et 110,5°Est; au-dessus du Pacifique, trois satellites entre les 174°Est et 180°Est. L'existence de plusieurs satellites au-dessus de l'Atlantique permet de faire face aux besoins importants de communications dans cette zone.

INTERSPUTNIK[33]

En 1971, l'organisation internationale de communications satellitaires INTERSPUTNIK a été créée par neuf pays; il s'agissait d'une agence de l'ex-Union soviétique, dont la mission était similaire à celle d'INTELSAT. Aujourd'hui, INTERSPUTNIK est une organisation interétatique, dont peut être membre le gouvernement de n'importe quel pays. Elle compte désormais 24 États membres (notamment l'Allemagne) et quelque 40 utilisateurs (entre autres, la France et le Royaume-Uni), qui sont représentés par leurs administrations postales ou par leurs organisations des télécommunications. Son siège est à Moscou.

Les télécommunications sont acheminées sur les bandes C et Ku (cf. infra).

Différents satellites (Gorizont, Express, Express A de la Fédération de Russie, et LMI-1 de l'entreprise commune Lockhead-Martin) couvrent également l'ensemble de la planète: un satellite orbite au-dessus de la zone atlantique et un deuxième est prévu; dans la zone de l'océan Indien, il y a trois satellites, et dans la zone pacifique, deux (cf. tableau, chapitre 5, point 5.3).

INMARSAT[34]

Depuis 1979, INMARSAT (Organisation internationale des télécommunications maritimes par satellites) assure dans le monde entier des communications **mobiles** en mer, dans l'air et sur terre, ainsi qu'un service d'appels de détresse. INMARSAT a été mis en place en tant qu'organisation interétatique à l'initiative de l'Organisation maritime internationale. INMARSAT, aujourd'hui privatisée, a son siège à Londres.

Le système INMARSAT repose sur neuf satellites placés sur orbite géostationnaire. Quatre des satellites – qui appartiennent à la génération INMARSAT-III – couvrent l'ensemble de la planète jusqu'aux régions polaires les plus extrêmes. Chacun d'eux couvre environ un tiers de la surface terrestre. De par leur position au-dessus des quatre régions océaniques (Atlantique occidental et oriental, Pacifique, océan Indien), ils permettent une couverture planétaire. De plus, chaque satellite INMARSAT dispose également d'un certain nombre de faisceaux étroits, ce qui permet de concentrer l'énergie sur des zones où les besoins de communications sont importants.

Les télécommunications sont acheminées sur les bandes L et Ku (cf. infra, point 4.2.4).

[33] Page d'accueil d'INTERSPUTNIK: http://www.intersputnik.com.
[34] Page d'accueil d'INMARSAT, http://www.inmarsat.com

PANAMSAT [35]

PanAmSat a vu le jour en 1988 en tant qu'opérateur commercial d'un système de satellites mondial ayant son siège aux États-Unis. Aujourd'hui, il dispose d'une flotte de 21 satellites fournissant différents services de télévision et de télécommunication dans le monde entier, mais principalement aux États-Unis.

Les télécommunications sont acheminées sur les bandes C et Ku.
Sept des vingt-et-un satellites couvrent la zone atlantique, deux la pacifique et deux l'indienne. La couverture des autres satellites s'étend à l'Amérique (Nord et Sud). Ces satellites ne jouent qu'un rôle mineur en ce qui concerne les communications en Europe.

4.2.3.2. Systèmes de satellites régionaux

Les zones d'empreinte des faisceaux des systèmes satellitaires régionaux couvrent différentes régions et différents continents. Les communications ainsi acheminées ne peuvent donc être reçues que dans ces régions.

EUTELSAT[36]

EUTELSAT a été créée en 1977 par dix-sept administrations postales européennes aux fins de couvrir les besoins spécifiques de l'Europe dans le domaine des communications par satellite et de soutenir l'industrie aérospatiale européenne. EUTELSAT, qui compte quelque quarante États membres, a son siège à Paris. L'organisation doit être privatisée en 2001.

EUTELSAT dispose de dix-huit satellites géostationnaires, qui couvrent l'Europe, l'Afrique et une grande partie de l'Asie, et qui assurent une liaison avec l'Amérique. Les satellites sont situés entre 12,5°Ouest et 48°Est. EUTELSAT offre essentiellement des services télévisuels (850 canaux numériques et analogiques) et radiophoniques (520 canaux), tout en assurant également des services de communications, avant tout en Europe (y compris en Russie): par exemple, pour des vidéoconférences, des réseaux privés de grandes entreprises (entre autres, General Motors et Fiat), des agences de presse (Reuters, AFP), des fournisseurs de services financiers et des services mobiles de transmission de données.

Les télécommunications sont acheminées sur la bande Ku.

ARABSAT[37]

ARABSAT est le pendant d'EUTELSAT dans la région arabe. L'organisation, qui a été créée en 1976, a pour membres 21 pays arabes. Les satellites d'ARABSAT sont utilisés tant pour la transmission télévisuelle que pour les communications.

Les télécommunications sont acheminées essentiellement dans la bande C.

[35] Page d'accueil de PANAMSAT, http://www.panamsat.com
[36] Page d'accueil d'EUTELSAT: http://www.eutelsat.com.
[37] Page d'accueil d'ARABSAT: http://www.arabsat.

PALAPA[38]

Le système indonésien PALAPA, qui est exploité depuis 1995, est le pendant sud-asiatique d'EUTELSAT. Son faisceau d'empreinte couvre la Malaisie, la Chine, le Japon, l'Inde, le Pakistan et d'autres pays de la région.

Les télécommunications sont acheminées sur les bandes C et Ku.

4.2.3.3. Systèmes de satellites nationaux[39]

De nombreux pays utilisent, pour couvrir leurs besoins nationaux, leurs propres systèmes de satellites, dont les zones d'empreinte sont limitées.

Le satellite français de télécommunications **TELECOM** sert notamment à relier les départements français d'Afrique et d'Amérique du Sud avec la métropole. Les télécommunications sont acheminées sur les bandes C et Ku.

ITALSAT dispose de satellites de télécommunications, dont les zones d'empreinte limitées, mais limitrophes, couvrent l'ensemble de la botte italienne. Aussi une réception n'est-elle possible qu'en Italie. Les télécommunications sont acheminées sur la bande Ku.

AMOS est un satellite israélien dont la zone d'empreinte couvre le Moyen-Orient. Les télécommunications sont acheminées sur la bande Ku.

Les satellites espagnols de **HISPASAT** couvrent l'Espagne et le Portugal (traces Ku) et servent à transmettre des programmes de télévision vers l'Amérique du Nord et l'Amérique du Sud.

4.2.4. Attribution de fréquences

La répartition des fréquences est de la compétence de l'Union internationale des télécommunications (ITU). Pour assurer un certain ordre, le monde a été divisé pour les communications hertziennes en trois régions:

1. Europe, Afrique, ex-Union soviétique, Mongolie,

2. Amérique du Nord et Amérique du Sud, Groenland y compris,

3. Asie, exception faite des pays de la région 1, Australie et Pacifique Sud.

Cette répartition traditionnelle a été conservée pour les communications par satellites; elle est à l'origine d'une concentration de satellites dans certaines zones géostationnaires. Les principales bandes de fréquence pour les communications par satellites sont les suivantes:

- la bande L (0,4 – 1,6 GHz) pour les communications mobiles par satellites, par exemple via INMARSAT,

[38] *Hans Dodel*, Satellitenkommunikation, Hüthig Verlag, 1999.
[39] *Hans Dodel,* Satellitenkommunikation, Hüthig Verlag, 1999 et recherches Internet.

- la bande C (3,6 - 6,6 GHz) pour les stations hertziennes terrestres, par exemple via INTELSAT,

- la bande Ku (10 - 20GHz) pour les stations hertziennes terrestres, par exemple INTELSAT-Ku-Spot et EUTELSAT,

- la bande Ka (20 - 46 GHz) pour les stations hertziennes terrestres, par exemple les satellites de communication militaires (v.4, 4.3.),

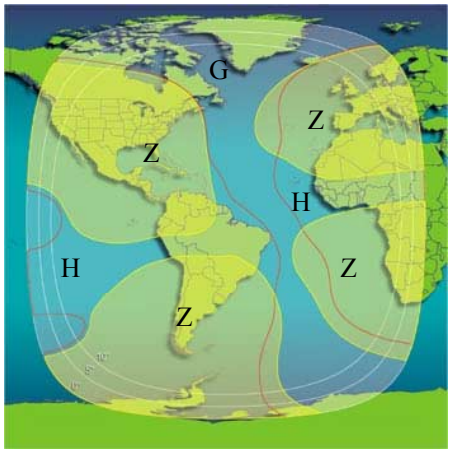
- la bande V (46 – 56 GHz) pour les microstations hertziennes (VSAT).

4.2.5. Zones couvertes par les satellites (empreintes au sol)

Par zone d'empreinte, on entend la région de la terre qui est couverte par une antenne de satellite. Cette zone peut représenter jusqu'à 50% de la surface terrestre ou, lorsque le signal est concentré, des points régionaux plus petits.

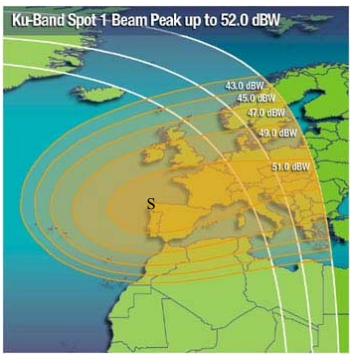
Plus la fréquence du signal émis est élevée, plus il est possible de le concentrer, et plus la zone d'empreinte peut être réduite. La concentration du signal satellitaire émis sur des zones d'empreinte plus petites permet d'augmenter l'énergie du signal. Ainsi, plus la zone d'empreinte est petite, plus le signal peut être fort, et, partant, plus l'antenne de réception peut être réduite.

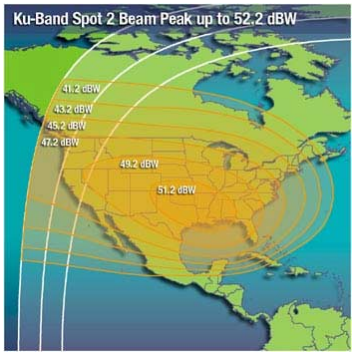
En résumé, la situation se présente précisément comme suit pour les satellites d'INTELSAT[40]:

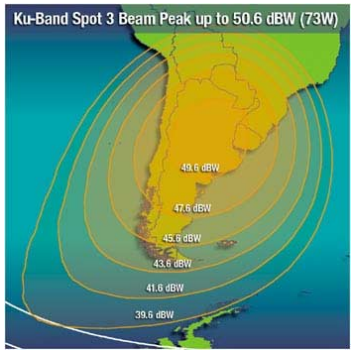


Les zones d'empreinte des satellites d'INTELSAT se répartissent entre différents faisceaux:
Le faisceau à couverture mondiale (G) de tout satellite couvre environ un tiers de la surface terrestre.
Les faisceaux à semi-couverture (H) couvrent une surface légèrement inférieure à la moitié de celle du faisceau à couverture mondiale Les faisceaux zonaux (Z) représentent des zones de réception dans certaines parties du monde; ils sont plus petits que les faisceaux à semi-couverture. Il y a enfin ce qu'il est convenu d'appeler les pinceaux, c'est-à-dire des zones d'empreinte précises et réduites(cf. infra).

[40] INTELSAT Satellit 706, 307°E, Ausleuchtzonen von Homepage von INTELSAT: http://www.intelsat.com







Les fréquences de la bande C concernent les faisceaux à couverture mondiale, les faisceaux à semi-couverture ainsi que les faisceaux zonaux. Les fréquences de la bande Ku sont utilisées dans les faisceaux étroits.

4.2.6. Dimensions des antennes requises pour une station terrienne

Les antennes de réception terrestres sont des antennes paraboliques dont la limite va de 0,5 à 3 m. Le miroir parabolique reflète toutes les ondes captées et les concentre en un point focal. C'est à cet endroit précis que se trouve le système de réception proprement dit. Plus l'énergie du signal au point de réception est grande, plus le diamètre de l'antenne parabolique peut être réduit.

Ce qui est déterminant pour le but poursuivi dans le contexte de l'enquête réalisée pour le présent rapport, c'est qu'une partie des communications intercontinentales sont acheminées via la bande C dans les faisceaux à couverture mondiale des satellites d'INTELSAT et d'autres satellites (par exemple, INTERSPUTNIK), et que pour leur réception des antennes d'un diamètre de l'ordre de 30 m sont parfois nécessaires (cf. chapitre 5). Des antennes de 30 m étaient également nécessaires pour les premières stations de réception des satellites de communications, dès lors que la première génération d'INTELSAT n'utilisait que des faisceaux à couverture mondiale et que la transmission des signaux était encore bien moins perfectionnée qu'aujourd'hui. Ces panneaux d'un diamètre parfois supérieur à 30 m sont encore utilisés aujourd'hui dans les stations en question, même si, techniquement, ils ne sont plus nécessaires (v. aussi 5, 5.2.3).

Les antennes actuellement nécessaires pour les communications INTELSAT dans la bande C ont un diamètre compris entre 13 et 20 m.

Pour les traces Ku des satellites d'INTELSAT ainsi que pour d'autres satellites (bande Ku d'EUTELSAT, bande Ku AMOS, etc.), le diamètre des antennes nécessaires est compris entre 2 et 15 m.

Pour les microstations, qui fonctionnent dans la bande V, et dont les signaux sont plus concentrés encore que dans la bande Ku, compte tenu de la fréquence élevée, un diamètre d'antenne compris entre 0,5 et 3,7 m est suffisant (p.ex., VSAT d'EUTELSAT ou INMARSAT).

4.3. Communications par satellite à finalités militaires

4.3.1. Généralités

Dans le domaine militaire aussi, les satellites de communication jouent un rôle important. De nombreux pays – notamment les États-Unis, le Royaume-Uni, la France et la Russie – exploitent des satellites de communication militaires géostationnaires qui rendent possibles les communications mondiales indépendamment d'autres vecteurs. Avec 32 positions orbitales, les États-Unis disposent d'un satellite tous les 10° en moyenne. Il est parfois fait usage aussi de satellites commerciaux géostationnaires pour des communications militaires.

4.3.2. Fréquences utilisées par les militaires

Les bandes utilisées pour les communications militaires vont de 4 GHz à 81 GHz. Les bandes utilisées par les satellites militaires sont plus particulièrement la bande X (SHF), 3-30 GHz, et la bande Ka (EHF), 20-46 GHz.

4.3.3. Taille des stations de réception

Celles-ci sont mobiles, leur taille ne dépassant pas alors dans certains cas quelque dizaines de centimètres, ou stationnaires – dans ce cas, leur diamètre n'est pas supérieur à 11 mètres. On compte cependant deux types d'antennes (réception de satellites DSCS) d'un diamètre de 18 mètres.

4.3.4. Exemples

Le programme américain **MILSTAR** (Military Strategy, Tactical and Relay Satellite System) utilise 6 satellites géostationnaires. Il permet à l'armée des États-Unis de faire communiquer entre eux et avec les commandements, au moyen de petits postes, les avions, les navires et les troupes. L'interconnexion des satellites assure la disponibilité continue, même en cas de défaillance de l'ensemble des stations non américaines au sol.

Le **DSCS** (Defense Satellite Communications System) permet également des communications mondiales grâce à 5 satellites géostationnaires. Il est utilisé par les militaires et par certains services gouvernementaux.

Le système militaire britannique **SKYNET** est également un système mondial.

Le système français **SYRACUSE**, le système italien **SICRAL** et le système espagnol "empruntent" des satellites de communication civils et permettent des communications militaires dans la bande X, mais limitées au plan régional.

Les Russes assurent leurs communications militaires par transpondeur sur la bande X grâce à leurs satellites Molnyia.

L'OTAN exploite ses propres satellites (**NATO IIID, NATO IVA** et **IVB**). Ils transmettent communications vocales, télex et données entre les différentes unités.

5. Preuves par indices de l'existence d'au moins un système d'interception mondial

5.1. Pourquoi une preuve par indices?

Naturellement, les services secrets ne font pas publiquement état de leurs activités. Aussi ne faut-il pas, en tout état de cause, espérer trouver une déclaration officielle dans laquelle les services de renseignement étranger des pays UKUSA reconnaîtraient coopérer à l'exploitation d'un système d'interception mondial. Dès lors, la preuve doit être établie en réunissant un nombre maximal d'indices, pour constituer une preuve convaincante.

La chaîne des indices qui formeraient une telle preuve se compose de trois éléments:

- la preuve que les services de renseignement étranger des pays UKUSA interceptent des communications privées et commerciales;

- la preuve de la découverte des différentes stations d'interception terrestres – indispensables compte tenu du fonctionnement du système de communication civil par satellites – gérées par les pays UKUSA;

- la preuve qu'il existe entre ces pays une coopération des services de renseignement allant au-delà de ce qui est courant. Que cette coopération aille jusqu'à l'acceptation par les partenaires de contrats d'interception et à la communication directe par ceux-ci du matériel brut intercepté, sans aucune forme d'exploitation propre, voilà qui n'a aucune espèce d'importance pour la preuve de l'existence d'une coopération. Cela ne joue un rôle que pour la question de savoir quelles sont les hiérarchies dans le contexte de cette coopération d'interception.

5.1.1. Preuve de l'activité d'interception des services de renseignements étrangers

Dans les démocraties, à tout le moins, les services de renseignement exercent leurs activités sur la base de lois, qui énoncent leurs objectifs et/ou leurs pouvoirs. Aussi est-il simple de prouver qu'il existe dans nombre de ces pays des services de renseignement étranger, qui interceptent les communications civiles. Tel est également le cas des cinq pays UKUSA mentionnés, qui disposent de tels services. Pour chacun de ces pays, il ne faut pas apporter une preuve supplémentaire spécifique de l'interception des communications à destination ou en provenance de leur territoire. Sur leur territoire, ils peuvent également capter, dans le cas de communications par satellite, une partie des messages dont les destinataires se trouvent à l'étranger. Dans aucun des cinq pays UKUSA, nulle disposition légale n'empêche les services concernés d'agir ainsi. La logique interne de la méthode du contrôle stratégique des télécommunications extérieures et le but de ce contrôle, du moins celui qui en partie connu, obligent à considérer que lesdits services agissent bien ainsi.[41]

[41] Votre rapporteur dispose d'informations le prouvant. La source est protégée.

5.1.2. Preuve de l'existence de stations dans les zones géographiques requises

La seule limite à laquelle se heurte la tentative d'exercer une surveillance sur les communications effectuées par satellite procède de la technique même de ce moyen de communication. Il n'existe aucun endroit à partir duquel il serait possible de capter **toutes les** communications par satellite dans le monde entier (cf. chapitre 4, point 4.2.5).

Un système d'interception fonctionnant au niveau mondial pourrait être mis en place pour autant que les trois conditions suivantes existent:

- l'exploitant a une partie de son territoire dans toutes les régions du monde requises;

- l'exploitant a, dans une certaine mesure, une partie de son territoire dans toutes les régions du monde requises et, en plus, un droit d'hospitalité dans les parties du monde qui lui font défaut, et il peut y exploiter des stations ou utiliser celles de son hôte;

- l'exploitant est une association d'États dans le domaine du renseignement et utilise le système dans les régions du monde nécessaires à cet effet.

Aucun des pays UKUSA ne serait en mesure d'exploiter seul un système mondial. À tout le moins officiellement, les États-Unis n'ont aucune colonie. De même, le Canada, l'Australie et la Nouvelle-Zélande n'ont aucune partie de leur territoire située à l'extérieur de leurs frontières au sens propre. Le Royaume-Uni ne pourrait, lui non plus, exploiter seul un système d'interception mondial (cf. chapitre 6).

5.1.3. Preuve d'une association étroite entre les services de renseignements

Il n'est pas possible de dire, par contre, si et dans quelle mesure les pays UKUSA collaborent dans le secteur des services de renseignement. D'ordinaire, une collaboration entre ces services est d'ordre bilatéral et prend la forme d'un échange du matériel exploité. Une association multilatérale est en soi déjà quelque chose de très exceptionnel; s'il faut encore y ajouter un échange régulier de matériel brut, alors nous sommes en présence d'un phénomène entièrement nouveau. L'existence d'une association de ce type ne peut être établie que sur la base d'indices.

5.2. Comment reconnaît-on une station d'interception des communications par satellite?

5.2.1. Critère 1: accès de l'installation

Les installations de la poste, de la radiotélévision ou des instituts de recherche disposant de grandes antennes sont accessibles aux visiteurs, au moins sur rendez-vous. Les stations d'interception ne le sont pas, par contre. La plupart du temps, elles sont gérées officiellement par des militaires, qui assurent également une partie au moins de l'interception. Ainsi, dans les stations gérées par les États-Unis, par exemple, c'est le Naval Security Group (NAVSECGRU) ou l'Air Intelligence Agency des forces aériennes américaines (AIA) ou le United States Army Intelligence and Security Command (INSCOM) qui assure avec la NSA le fonctionnement des stations. Dans les stations britanniques, c'est la Royal Airforce qui gère les installations avec le service de renseignement britannique (GCHQ). Ces dispositions garantissent un contrôle

militaire strict de l'installation, tout en permettant de camoufler les activités.

5.2.2. Critère 2: type d'antenne

Dans les installations conformes au critère 1, il existe différents types d'antennes, pouvant se distinguer en fonction de leur structure caractéristique. Leur forme donne des indications quant au but poursuivi par l'installation d'interception. Ainsi, des rangées d'antennes verticales formant un cercle de grand diamètre (antennes Wullenweber) sont utilisées pour déterminer l'orientation de signaux hertziens. De même, une succession circulaire d'antennes rhomboïdales (antennes dites en râteau) sont utilisées dans le même but. Des antennes de réception multidirectionnelles ou antennes directionnelles, comparables à des antennes de télévision classiques gigantesques, servent pour intercepter des signaux hertziens non dirigés. **Pour la réception de signaux satellitaires, on utilise en revanche exclusivement des antennes paraboliques.** Lorsque les antennes paraboliques sont situées à découvert, il est possible de calculer, en connaissant leur situation, leur angle d'inclinaison (élévation) et leur orientation (azimut) le satellite dont les émissions sont interceptées. Il serait possible de le faire, par exemple, à Morwenstow (Royaume-Uni) ou à Yakima (États-Unis) ou à Sugar Grove (États-Unis). La plupart du temps, les antennes paraboliques sont cependant dissimulées sous des enveloppes sphériques blanches, appelées radômes. Ces enveloppes servent non seulement à protéger les antennes mais aussi à cacher leur orientation.

Si des antennes paraboliques ou des radômes se trouvent sur le site d'une station d'interception, alors, on peut être sûr que des signaux provenant de satellites y sont captés. Ce qui ne nous dit toujours pas de quel genre de signaux il s'agit en l'occurrence.

5.2.3. Critère 3: dimension de l'antenne

Dans une installation conforme au critère 1, les antennes de réception des satellites peuvent être utilisées dans les buts suivants:

- stations de réception des satellites de communication militaires,
- stations de réception des satellites-espions (photos, radar)
- stations de réception des satellites SIGINT
- stations de réception servant à l'interception des satellites de communications civils.

Il n'est pas possible de déduire la mission que remplissent les antennes/radômes à partir de leur aspect extérieur. Toutefois, leur diamètre fournit certaines indications à cet égard. Pour les satellites de communication civils destinés à recevoir le faisceau à couverture mondiale dans la bande C des communications internationales civiles par satellites, il existe des dimensions minimales, fonction de la technique. Pour la première génération de ces satellites, des antennes d'un diamètre de l'ordre de 25 à 30 m étaient nécessaires; aujourd'hui, un diamètre compris entre 15 et 20 m est suffisant. Le filtrage automatique des signaux captés par ordinateur requiert une qualité optimale du signal; aussi, lorsque le renseignement est l'objectif, opte-t-on pour une antenne de la dimension maximale.

Pour les communications militaires, on observe dans les centres de commandement deux types d'antennes dont le diamètre est proche de 18 m (AN/FSC-78 et AN/FSC-79). La plupart des antennes destinées aux communications militaires ont toutefois un diamètre beaucoup plus faible étant donné qu'elles doivent être transportables (stations tactiques).

Les stations au sol destinées aux satellites SIGINT ne nécessitent que de petites antennes, ce qui s'explique par les caractéristiques du signal renvoyé à la station (faisceau et fréquence importants). Cela concerne aussi les antennes captant les signaux de satellites d'espionnage.

Si une installation présente au moins deux antennes pour satellites de plus de 18 m, il est certain que l'interception des communications civiles y est pratiquée. S'agissant d'une station accueillant des militaires des États-Unis, une des antennes peut servir aux communications militaires.

5.2.4. Critère 4: Preuves officielles

Pour certaines stations, on dispose d'une description officielle précise des missions. Les sources sont considérées comme officielles s'il s'agit d'informations gouvernementales ou d'informations fournies par les militaires.
S'il est satisfait à ce critère, il n'est pas nécessaire d'examiner les autres pour classer une station parmi les stations d'interception de communications civiles.

5.3. Données, pouvant être obtenues par chacun, concernant les stations d'interception connues

5.3.1. Méthode

Afin de déterminer quelles stations répondent aux critères énoncés au point 5.2 et font partie du système d'interception mondial et de préciser de quelles missions elles sont chargées, la documentation afférente, parfois contradictoire (Hager[42], Richelson[43], Campbell[44]), les documents déclassés[45], la page d'accueil de la Federation of American Scientists[46] ainsi que les pages d'accueil de NSA, AIA, etc. et d'autres publications sur Internet ont été consultés[47]. Pour la station néo-zélandaise de Waihopai, on dispose d'une description officielle de ses missions

---

42 *Nicky Hager*: Exposing the global surveillance system. http://www.ncoic.com/echelon1.htm
Nicky Hager: Secret Power. New Zealands´s Role in the international Spy Network, Craig Potton Publishing 1996.

43 *Jeffrey T. Richelson*, Desperately Seeking Signals, The Bulletin of the Atomic Scientists Vol 56 Nr. 2,47-51, http://www.bullatomsci.org/issues/2000/ma00/ma00richelson.html
Jeffrey T. Richelson, The U.S. Intelligence Community, Westview Press 1999.

44 *Duncan Campbell*, dans PE 168.184 (octobre 1999)
http://www.europarl.eu.int/dg4/stoa/en/publi/pdf/98-14-01-2en.pdf
Duncan Campbell: Inside Echelon, 25.7.2000http://www.heise.de/tp/deutsch/special/ech/6928/1.html
Duncan Campbell: Interception Capabilities n- Impact and Exploitation – Echelon and its role in COMINT, présenté à la commission Echelon du Parlement européen le 22 janvier 2001
Federation of American Scientists, http://www.fas.org/irp/nsa/nsafacil.html .

45 *Jeffrey T. Richelson*: Newly released documents on the restrictions NSA places on reporting the identities of US-persons: Declassified: http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB23/index.html .

46 Federation of American Scientists (FAS), http://www.fas.org/ .

47 Military.com; *.mil-Homepages.

fournie par la gouvernement du pays[48]. En outre, les zones de couverture des satellites de communication ont été rassemblées, les dimensions des antennes nécessaires calculées et reportées sur des planisphères, de même que les stations possibles.

5.3.2. Analyse approfondie

L'analyse tient compte des principes ci-après, qui sont liés à la physique de la communication par satellite (voir également chapitre 4):

- Une antenne ne peut capter que ce qui se trouve dans la zone de couverture où elle est située. Pour pouvoir recevoir des communications relevant principalement des bandes C et Ku, une antenne doit se trouver à l'intérieur de la zone de couverture couvrant les bandes C et Ku.
- Il faut une antenne pour chaque faisceau à couverture mondiale, même si les faisceaux de deux satellites se recoupent.
- Si un satellite présente plus de zones de couverture que le faisceau mondial (c'est le cas de la génération de satellites actuelle), une seule antenne ne permet pas de capter toutes les communications transitant par ces satellites étant donné qu'une seule antenne ne peut se situer dans toutes les zones de couverture des satellites. Pour capter le faisceau à semi-couverture et le faisceau mondial d'un satellite, il faut donc deux antennes dans deux régions différentes (voir schéma des zones de couverture au chapitre 4). Si d'autres faisceaux s'ajoutent à cela (zonaux et pinceaux), des antennes supplémentaires sont nécessaires. Les différents faisceaux d'un même satellite qui se recoupent peuvent en principe être captés par une seule antenne, car il est techniquement possible de séparer différentes bandes de fréquence à la réception, mais cela est à l'origine d'une dégradation du rapport signal/bruit.

Pour le reste, les conditions énoncées au point 5.2. sont d'application: les installations ne sont pas accessibles étant donné qu'elles sont exploitées par les militaires[49]; la réception de signaux satellite suppose des antennes paraboliques; la taille des antennes destinées à capter la bande C du faisceau mondial pour la première génération INTELSAT est supérieure à 30 mètres, pour les autres générations, supérieure à 15-18 m. Les descriptions officielles d'une partie des stations sont considérées comme preuves du rôle d'interception de ces stations.

5.3.2.1. Le parallélisme entre le développement des INTELSAT et la construction de stations

Tout système d'écoute global doit croître au rythme du progrès des communications. Le début des communications par satellite doit donc donner lieu à l'apparition des premières stations, et la mise en service de nouvelles générations de satellites à la construction de nouvelles stations et de nouvelles antennes satellitaires opérationnelles. Le nombre des stations et des antennes satellitaires doit augmenter chaque fois que l'interception des communications l'exige.

---

[48] Domestic and External Security Secretariat, Department of the Prime Minister and Cabinet, Securing our Nation's Safety (2000), http://www.dmpc.govt.nz/dess/securingoursafety/index.html .

[49] Abréviations utilisées: NAVSECGRU: Naval Security Group, INSCOM: United States Army Intelligence And Security Command, AIA: Air Intelligence Agency, IG: Intelligence Group, IS: Intelligence Squadron, IW: Intelligence Wing, IOG: Information Operation Group, MIG: Military Intelligence Group.

Par conséquent, à l'inverse, lorsque l'on crée de nouvelles zones de couverture et que l'on construit de nouvelles stations et de nouvelles antennes satellitaires, cela n'est pas par hasard: on peut voir là l'indice de l'existence d'une station d'écoute de communications.

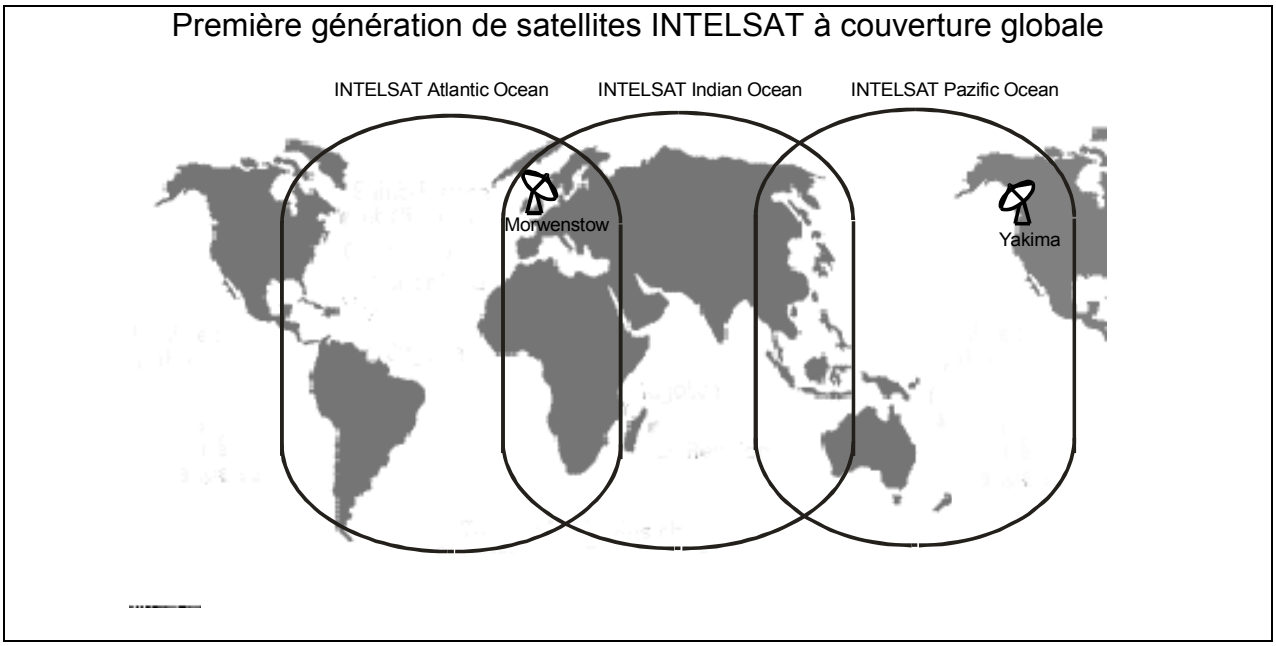
Étant donné que les satellites INTELSAT étaient les premiers satellites de communication et que, de plus, ils couvraient la planète tout entière, il est logique que la mise en place et l'agrandissement de stations suivent le développement des générations d'INTELSAT.

La première génération mondiale

C'est dès 1965 que le premier satellite INTELSAT (Early Bird) fut mis en orbite géostationnaire. Il avait une capacité de transmission encore faible et ne couvrait que l'hémisphère nord.

Avec les générations INTELSAT II et III, mises en service respectivement en 1967 et en 1968, on obtint, pour la première fois, une couverture globale. Les g*lobal beams* des satellites couvraient les zones atlantique, pacifique et indienne. Il n'y avait pas encore de zones de couverture plus petites. Pour capter la totalité des communications, il fallait donc trois satellites. Comme deux des g*lobal beams* se chevauchaient au-dessus de l'espace européen, il était possible, dans cette zone, grâce à une station munie de deux antennes satellitaires orientées différemment, de saisir les zones de couverture globales des deux satellites.

Première génération de satellites INTELSAT à couverture globale

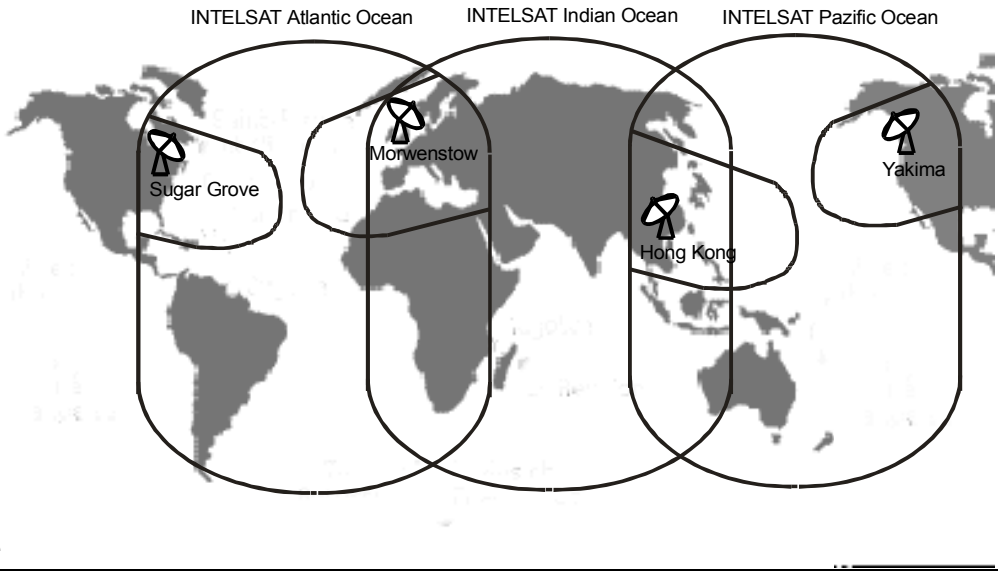


Au début des années 1970, **Yakima** fut créée dans le nord-ouest des États-Unis; en 1972/1973, **Morwenstow** fut créée dans le sud de l'Angleterre. Yakima disposait alors d'une grande antenne (orientée vers le Pacifique); Morwenstow avait deux grandes antennes (l'une orientée vers l'Atlantique, l'autre vers l'océan Indien). La localisation des deux stations permettait de capter la totalité des communications.

La deuxième génération mondiale

Les satellites INTELSAT de la deuxième génération (IV et IVA) furent développés dans les années 70 et mis en orbite géostationnaire (1971 et 1975). Les nouveaux satellites, qui assuraient aussi une couverture globale et disposaient de beaucoup plus de canaux radio (4000-6000), avaient aussi, outre les g*lobal beams*, des z*one beams* dans l'hémisphère nord (voir chapitre 4). Un z*one beam* couvrait l'est des États-Unis, un autre l'ouest des États-Unis, un autre encore l'Europe occidentale et un dernier l'Asie de l'est. Dès lors, deux stations munies de trois antennes satellitaires ne permettaient plus de capter la totalité des communications. La station de Yakima couvrait le z*one beam* de "Ouest des États-Unis"; Morwenstow couvrait le z*one beam* "Europe". Pour couvrir les deux autres z*one beams*, il fallait disposer d'une station à l'est des États-Unis et d'une autre dans la région est-asiatique.

Deuxième génération de satellites INTELSAT à couverture mondiale



À la fin des années 70, **Sugar Grove** fut construite dans l'est des États-Unis (la station existait déjà pour écouter les communications russes); elle entra en service en 1980. Toujours dans la fin des années 70, une station fut mise en place à **Hong-Kong**. Dès lors, dans les années 80, les quatre stations – Yakima, Morwenstow, Sugar Grove et Hong-Kong – permettaient l'écoute globale des communications INTELSAT.

Les satellites INTELSAT ultérieurs, avec z*one beams* et s*pot beams* en plus des g*lobal beam* et des *hemi beams*, nécessitèrent la mise en place de nouvelles stations dans différentes parties du monde. Arrivés à ce point, il est très difficile d'établir un lien entre la création de nouvelles stations et/ou l'installation de nouvelles antennes satellitaires sur la base des informations disponibles.

Comme, de plus, on a beaucoup de mal à obtenir des informations concernant les stations, il est impossible de savoir précisément quels satellites, avec quels *beams*, sont captés par quelle

station. Toutefois, on peut déterminer dans quels *beams* se trouvent des stations connues.

5.3.2.2. La couverture globale par stations qui écoutent manifestement des satellites de communication

À l'heure actuelle, les communications globales par satellite sont assurées par des satellites INTELSAT, INMARSAT et INTERSPUTNIK. Comme dans le cas des premières générations de satellites, la répartition en trois zones de couverture (zones indienne, pacifique et atlantique) est maintenue. Dans chacune des zones de couverture, on trouve des stations qui répondent aux critères caractéristiques des stations d'écoute.

Satellites en orbite au-dessus de l'océan Indien

INTELSAT 604 (60°E), 602 (62°E), 804 (64°E), 704 (66°E) EXPRESS 6A (80°E) INMARSAT zone indienne	Geraldton, Australie Pine Gap, Australie Morwenstow, Royaume-Uni Menwith Hill, Royaume-Uni
INTELSAT APR1 (83°), APR-2 (110,5°)	Geraldton, Australie Pine Gap, Australie Misawa, Japon

Satellites en orbite au-dessus du Pacifique

INTELSAT 802 (174°), 702 (176°), 701 (180°) GORIZONT 41 (130°E), 42 (142°E), LM-1 (75°E) INMARSAT zone pacifique	Waihopai, Nouvelle-Zélande Geraldton, Australie Pine Gap, Australie Misawa, Japon Yakima, États-Unis: uniquement Intelsat et Inmarsat

Satellites en orbite au-dessus de l'Atlantique

INTELSAT 805 (304,5°), 706 (307°), 709 (310°) 601 (325,5°), 801 (328°), 511(330,5°), 605 (332,5°), 603 (335,5°), 705 (342°) EXPRESS 2 (14°W), 3A (11°W) INMARSAT zone atlantique	Sugar Grove, États-Unis Sabana Seca, Puerto Rico Morwenstow, Royaume-Uni Menwith Hill, Royaume-Uni
INTELSAT 707 (359°)	Morwenstow, Royaume-Uni Menwith Hill, Royaume-Uni

On voit donc qu'une écoute globale des communications est possible.
En outre, il existe encore d'autres stations qui, si elles ne répondent certes pas au critère de dimension d'antennes et pour lesquelles on ne dispose pas d'autres éléments concluants, peuvent cependant faire partie du système d'écoute global. Ces stations permettraient, par exemple, d'intercepter les z*ones beams* ou s*pot beams* de satellites dont les g*lobal beams* sont écoutés par d'autres stations ou pour les g*lobal beams* desquels il n'est pas nécessaire de disposer de grandes antennes satellitaires.

5.3.2.3. Les stations: détails

Pour la description détaillée des stations, on distingue entre, d'une part, stations qui écoutent manifestement des satellites de communication (critères de la section 5.2) et, d'autre part, stations dont la mission ne peut être prouvée sur la base des critères susmentionnés.

5.3.2.3.1. Stations destinées à l'écoute de satellites de communication

Les critères décrits à la section 5.2, qui peuvent être considérés comme indices de l'existence d'une station d'écoute de satellites de communication, sont aussi valables pour les stations suivantes:

Yakima, États-Unis (120°O, 46°N)
La station a été créée dans les années 1970, en même temps que la première génération de satellites. Depuis 1995, la Air Intelligence Agency (AIA) est sur place, avec le 544th Intelligence Group (Detachment 4). Le Naval Security Group (NAVSECGRU) y est également stationné. La station compte six antennes satellitaires, dont les sources ne permettent pas de connaître la dimension. Selon Hager, ce sont des antennes satellitaires de grande dimension et elles sont orientées sur des satellites Intelsat en orbite au-dessus du Pacifique (deux antennes satellitaires) et sur des satellites Intelsat en orbite au-dessus de l'Atlantique; des antennes sont orientées sur les satellites Inmarsat 2.

Le fait que Yakima a été créée en même temps que la première génération de satellites Intelsat, d'une part, et la description générale des missions du 544th Intelligence Group, d'autre part, donnent à penser que Yakima joue un rôle dans la surveillance globale des communications. Autre indice: Yakima est proche d'une station de réception de satellites normale, située à 100 miles au nord.

Sugar Grove, États-Unis (80°O, 39°N)
Sugar Grove a été créée en même temps qu'était mise en service la deuxième génération de satellites Intelsat, à la fin des années 70. Y sont stationnés le NAVSECGRU ainsi que l'AIA, avec le 544th Intelligence Group (Detachment 3). Selon plusieurs auteurs, la station compte dix antennes satellitaires, dont trois ont plus de 18 mètres (18,2 mètres, 32,3 mètres et 46 mètres) et conviennent donc clairement pour écouter des satellites de communication. À la station, une des missions du Detachment 3 du 544th IG est de fournir un "intelligence support" pour la collecte, par les stations de la Navy, d'informations provenant de satellites de communication[50].

De plus, Sugar Grove est située à proximité (60 miles) de la station de réception de satellites normale d'Etam.

Sabana Seca, Puerto Rico (66°O, 18°N)
En 1952, le NAVSECGRU fut stationné à Sabana Seca. Depuis 1995, s'y trouve aussi la AIA, avec le 544th IG (Detachment 2). La station compte au moins une antenne satellitaire d'un diamètre de 32 mètres et quatre autres antennes satellitaires de petite dimension.

Officiellement, les missions de la station sont: traitement des communications par satellite ("performing satellite communication processing"), "cryptologic and communications service" et appui à des missions de la Navy et du DoD (notamment, collecte d'informations COMSAT (d'après le 544th IG)). À l'avenir, Sabana Seca doit devenir la première station d'analyse et de traitement de communications par satellite.

Morwenstow, Royaume-Uni (4°O, 51°N)
Tout comme Yakima, Morwenstow a été créée en même temps que la première génération de satelllites Intelsat, au début des années 70. Morwenstow est desservie par le service de renseignements britannique (GCHQ). Morwenstow compte environ 21 antennes satellitaires, dont trois d'un diamètre de 30 mètres; on ne dispose pas de données concernant la dimension des

[50] „It provides enhanced intelligence support to Air Force operational commanders and other consumers of communications satellite information collected by Navy-commanded field stations.“ aus der Homepage der (44th Intelligence Group http://www.aia.af.mil .

autres antennes.

Par les sources officielles, on ne sait rien de la mission de la station. Mais la dimension et le nombre de ses antennes satellitaires ainsi que le fait qu'elle soit implantée à seulement 110 km de la station télécom de Goonhilly ne permettent aucun doute: il s'agit d'une station d'écoute de satellites de communication.

Menwith Hill, Royaume-Uni (2°O, 53°N)

Menwith Hill a été créée en 1956. En 1974, la station comptait déjà 8 antennes satellitaires. Depuis, on y trouve quelque 30 antennes satellitaires, dont plusieurs d'un diamètre supérieur à 20 mètres. Au moins une des grandes antennes, mais certainement pas l'ensemble de celles-ci, est une antenne de réception de communications militaires (AN/FSC-78). A Menwith Hill, Britanniques et Américains coopèrent. Pour les Américains, y sont stationnés le NAVSECGRU, la AIA (451st IOS) ainsi que l'INSCOM, qui a le commandement de la station. Le site de Menwith Hill appartient au ministère britannique de la Défense et est loué au gouvernement américain. Officiellement, la mission de Menwith Hill est: "to provide rapid radio relay and to conduct communications research". Selon Richelson et la Fédération des scientifiques américains, Menwith Hill est à la fois une station terrestre pour satellites d'espionnage et une station d'interception pour satellites de communications russes.

Geraldton, Australie (114°O, 28°S)

La station existe depuis le début des années 90. Elle est dirigée par les services secrets australiens (DSD); des Britanniques, précédemment stationnés à Hong Kong (voir plus haut), font à présent partie du personnel de la station. Selon Hager, quatre antennes satellitaires, de même diamètre (quelque 20 m), sont orientées vers des satellites en orbite au-dessus de l'océan Indien et vers des satellites en orbite au-dessus du Pacifique. Selon des experts entendus sous serment au Parlement australien, Geraldton écoute des satellites de communication civils[51].

Pine Gap, Australie (133°O, 23°S)

La station de Pine Gap a été créée en 1966. Elle est dirigée par les services secrets australiens (DSD); à peu près la moitié des quelque 900 personnes qui y sont stationnées sont des Américains de la CIA et du NAVSECGRU[52].

Pine Gap compte 18 antennes satellitaires, dont une d'un diamètre d'environ 30 mètres et une d'un diamètre d'environ 20 mètres. Selon des sources officielles et différents auteurs, cette station est, depuis le début, une station terrestre pour satellites SIGINT. La station contrôle et commande plusieurs satellites d'espionnage, dont elle capte, traite et analyse les signaux. Toutefois, la présence des grandes antennes satellitaires donne à penser que la station écoute aussi des satellites de communication, car les satellites SIGINT ne nécessitent pas des antennes satellitaires de grande dimension. Jusqu'en 1980, les Australiens étaient exclus du département d'analyse des signaux. Depuis, ils ont libre accès à toutes les parties de la station, à l'exception de la salle de cryptographie nationale des Américains.

[51] Proof Committee Hansard, Joint Standing Committee on Treaties, Reference: Pine Gap, 9 August 1999, Canberra, http://www.aph.gov.au/hansard.

[52] Proof Committee Hansard, Joint Standing Committee on Treaties, Reference: Pine Gap, 9 August 1999, Canberra, http://www.aph.gov.au/hansard.

Misawa, Japon (141°O, 40°N)
La station de Misawa est dotée depuis 1948 d'une antenne HFDF. Y sont stationnés des Japonais et des Américains. Pour les États-Unis, il y a le NAVSECGRU, l'INSCOM ainsi que certains groupes de la AIA (544th IG, 301st IS). Officiellement, Misawa est un "Cryptology Operations Center". Selon Richelson, Misawa permet d'écouter les satellites russes Molnyia ainsi que d'autres satellites de communication russes.

Waihopai, Nouvelle-Zélande (173°O, 41°S)[53]
Waihopai existe depuis 1989. Depuis, on y trouve une grande antenne d'un diamètre de 18 mètres; par la suite, on a ajouté une deuxième antenne. Selon Hager, les antennes sont orientées sur des Intelsat 701 en orbite au-dessus du Pacifique. La mission de Waihopai consiste d'après les indications officielles du GCSB (General Communications Security Bureau) à intercepter les communications par satellite, à décrypter et à traiter les signaux.[54]
Étant donné que la station ne dispose que de deux antennes pour satellites, le service secret néozélandais ne peut intercepter qu'une petite partie des communications dans l'espace pacifique. La station n'est intéressante qu'en liaison avec une autre station de la même zone. Hager cite généralement Geraldton, en Australie, comme "station soeur" de Waihopai.[55]

Hong Kong (22°N, 114°O)
Créée à la fin des années 70, en même temps que la deuxième génération d'Intelsat, la station était équipée de grandes antennes satellitaires. On ne dispose pas de données concernant les dimensions précises. En 1994, on a entamé le démantèlement de la station de Hong Kong. Les antennes ont été transférées en Australie. On ne sait pas quelle station a repris les missions d'Hong Kong: Geraldton, Pine Gap ou Misawa, au Japon. Ces missions pourraient avoir été réparties sur différentes stations.

5.3.2.3.2. Autres stations

S'agissant des stations ci-dessous, les critères susmentionnés ne permettent pas d'en déterminer clairement la fonction:

Leitrim, Canada (75°O, 45°N)
Leitrim fait partie d'un programme d'échanges entre unités militaires canadiennes et américaines. Selon la Navy, quelque 30 personnes y sont stationnées. En 1985, on y installa la première de quatre antennes satellitaires, dont les deux plus grandes ont un diamètre d'environ 12 mètres seulement (évaluation). Officiellement, la mission de la station est le "cryptologic rating" et l'écoute de communications diplomatiques.

Bad Aibling, Allemagne (12°O, 47°N)

---

[53] Domestic and External Security Secretariat, Department of the Prime Minister and Cabinet "Securing our Nation's Safety", décembre 2000, http://www.dpmc.gov.nz/dess/securingoursafety/index.html.

[54] Domestic and External Security Secretariat, Department of the Prime Minister and Cabinet "Securing our Nation's Safety", décembre 2000, http://www.dpmc.gov.nz/dess/securingoursafety/index.html: "In 1989,[...] the GCBS opened its satellite communications interception station at Waihopai, near Blenheim. [...] The signals intelligence is obtained from a variety of foreign communications and other non-communications signals, such as radar. The GCBS not only intercepts the signals, it also processes, decrypts or decodes and/or translates the information the signals contain before passing it on to the appropriate Minister or government department.".

[55] *Nicky Hager*, Secret Power, New Zealand's Role in the International Spy Network, Craig Potton Publishing (1996), 182.

La station est implantée à proximité de Bad Aibling. Y travaillent quelque 750 Américains. Sont stationnés à Bad Aibling l'INSCOM (66th IG, 718 IG), qui assure le commandement, le NAVSECGRU ainsi que divers groupes de l'AIA (402nd IG, 26th IOG). On trouve là 14 antennes satellitaires, dont aucune de plus de 18 mètres. Officiellement, Bad Aibling accomplit les missions suivantes: "rapid radio relay and secure commo, support to DoD and Unified Commands, medium and longhand commo HF& satellite, communication physics research, test and evaluate commo equipment". Selon Richelson, Bad Aibling est une station terrestre pour satellites SIGINT et pour l'interception de satellites de communication russes. Le 30 septembre 2002, la station devrait être fermée, en vertu d'une décision du ministère de la défense. Le personnel serait réparti sur d'autres unités.[56]

Ayios Nikolaos, Chypre (32°O, 35°N)

Ayios Nikolaos (Chypre) est une station britannique. Elle compte 14 antennes satellitaires, de grandeur inconnue. Ses missions sont réparties entre deux unités: "Signals Regiment Radio et Signals Unit (RAF)".

Sa proximité par rapport aux États arabes et le fait qu'elle est la seule station à être située à l'intérieur de plusieurs zones de couverture (notamment des *spot beams*) de la région donnent à penser que la station de Ayios Nikolaos joue un rôle important en matière d'obtention de renseignements.

Shoal Bay, Australie (134°O, 13°S)

Shoal Bay est une station desservie uniquement par le service australien de renseignements. La station compterait dix antennes satellitaires, dont les dimensions ne sont pas précisées. D'après des photographies, les cinq plus grandes ont un diamètre de 8 mètres maximum, et la sixième que l'on peut voir a un diamètre encore inférieur. Selon Richelson, les antennes sont orientées vers les satellites PALAPA indonésiens. La station ferait-elle partie du système global d'écoute des communications civiles? On l'ignore.

Guam, Pacifique (144°O, 13°S)

Guam existe depuis 1898. Elle abrite aujourd'hui une Naval Computer and Telecommunication Station, où sont stationnés le 544th IG de la AIA ainsi que des soldats de la Navy. La station compte au moins 4 antennes satellitaires, dont 2 de 15 m de diamètre.

Kunia, Hawaï (158°O, 21°N)

Depuis 1993, cette station est un Regional Security Operation Center (RSOC), desservi par le NAVSECGRU et l'AIA. Elle a notamment pour missions la mise à disposition d'informations et de communications, ainsi que le soutien cryptologique. La fonction de Kunia demeure peu claire.

Buckley Field, États-Unis, Denver Colorado (104°O, 40°N)

La station a été créée en 1972. Y sont stationnés le 544th IG (Det. 45). La station compte environ cinq antennes satellitaires, dont quatre d'un diamètre d'environ 20 mètres. Officiellement, la station a pour mission de collecter, d'exploiter et d'analyser des données obtenues grâce à des satellites SIGINT concernant les phénomènes nucléaires.

[56] Communication du 31.5.2001, Homepage d'INSCOM, http://www.vulcan.belvoir.army.mil/bas_to_close.asp.

Medina Annex, États-Unis, Texas (98°O, 29°N)
Tout comme Kunia, Medina – créée en 1993 – est un Regional Security Operation Center, qui est desservi par le NAVSECGRU et des unités de l'AIA. Ses missions concernent les Caraïbes.

Fort Gordon (81°O, 31°N)
Fort Gordon est aussi un Regional Security Operation Center. Il est desservi par l'INSCOM et l'AIA (702nd IG, 721st IB, 202nd IB, 31st IS). On n'est pas sûr de ses missions.

Fort Meade, États-Unis (76°O, 39°N)
Fort Meade est le quartier général de la NSA.

5.3.3. Résultats: résumé

Des données réunies en ce qui concerne les stations et les satellites, et des préalables exposés plus haut, on peut tirer les conclusions suivantes:

1. Dans chaque zone de couverture, il existe, pour au moins quelques-uns des g*lobal beams*, des stations d'écoute munies chacune d'au moins une antenne d'un diamètre supérieur à 20 mètres et desservies par des Américains ou des Britanniques et/ou où des Américains ou des Britanniques exercent des activités de renseignement.

2. Le développement des communications par INTELSAT et l'apparition simultanée de stations d'écoute correspondantes attestent l'orientation globale du système.

3. Certaines de ces stations ont pour mission, d'après les informations officielles, l'interception de satellites de communication.

4. Les données figurant dans les documents déclassifiés peuvent être considérées comme attestant l'existence des stations qui y sont mentionnées.

5. Certaines stations se trouvent simultanément dans des *beams* et/ou *spots* de plusieurs satelllites, de sorte qu'une grande partie des communications peut être interceptée.

6. Il existe quelques autres stations qui ne sont pas munies de grandes antennes, mais qui peuvent cependant faire partie du système, car elles sont capables de capter des communications en provenance des *beams* et *spots*. Là, il faut renoncer à l'indice de la dimension des antennes et recourir à d'autres indices.

7. Il est démontré que certaines des stations mentionnées se trouvent à proximité immédiate de stations terrestres régulières de satellites de communication.

5.4. L'accord UKUSA

On appelle accord UKUSA un accord SIGINT signé en 1948 par le Royaume-Uni, les États-Unis, l'Australie, le Canada et la Nouvelle-Zélande.

5.4.1. Genèse de l'accord UKUSA[57]

L'accord UKUSA est un prolongement de la coopération très étroite qui a uni les États-Unis et la Grande-Bretagne pendant la deuxième guerre mondiale et qui s'était esquissée dès la première guerre mondiale.

L'intiative visant à la création d'une allliance SIGINT fut prise par les Américains, en août 1940, lors d'une rencontre entre Américains et Britanniques, à Londres[58]. En février 1941, les crypto-analystes américains envoyèrent en Grande-Bretagne une machine à décoder (PURPLE). La coopération en matière de crypto-analyse débuta au printemps 1941[59]. La coopération entre services de renseignements fut renforcée par l'engagement commun des flottes dans l'Atlantique nord, à l'été 1941. En juin 1941, les Britanniques réussirent à casser ENIGMA, le code de la marine allemande.

L'entrée en guerre de l'Amérique renforça encore la coopération SIGINT. En 1942, des cryptologues américains de la "Naval SIGINT Agency" commencèrent à travailler au Royaume-Uni[60]. La communication entre les "U-Boot Tracking-Rooms" de Londres, de Washington, puis, à partir de 1943, de Ottawa (Canada) devint à ce point étroite que, selon les participants, elles travaillaient comme une organisation unique[61].

Le printemps 1943 vit la signature de l'accord BRUSA-SIGINT ainsi qu'un échange de personnel. Le contenu de l'accord, qui concerne notamment le partage du travail, est résumé dans les trois premiers paragraphes: échange de toute information provenant de la découverte, de l'identification et de l'écoute de signaux, ainsi que des algorythmes des codes et clés de cryptage. Les Américains étaient compétents pour le Japon; les Britanniques pour l'Allemagne et l'Italie[62].

---

[57] *Christopher Andrew*, "The making of the Anglo-American SIGINT Alliance" in *Hayden B*., *Peake*, *Samuel Halpern* (Eds), In the Name of Intelligence. Essays in Honor of *Walter Pforzheimer,* (NIBC Press 1994, 95 – 109.

[58] *Christopher Andrew*, The making of the Anglo-American SIGINT Alliance, ibidem, 99: "At a meeting in London on 31 August 1940 between the British Chiefs of Staff and the American Military Observer Mission, the US Army representative, Brigadier General George V. Strong, reported that ´it had recently been arranged in principle between the British and the United States Governments that periodic exchange of information would be desirable, and said that ´the time had come or a free exchange of intelligence´". (zitiert nach COS (40) 289, CAB 79/6, PRO. *Smith*, The Ultra Magic Deals, 38, 43f-4. *Sir F.H. Hinsley*, et al., British Intelligence in the Second World War, Vol. I, 312f).

[59] *Christopher Andrew*, The making of the Anglo-American SIGINT Alliance, ibidem, 100: "In the spring of 1941, Steward Menzies, the Chief of SIS, appointed an SIS liason officer to the British Joint Services Missin in Washington, Tim O´Connor, […], to advice him on cryptologic collaboration".

[60] *Christopher Andrew*, The making of the Anglo-American SIGINT Alliance, ibidem, 100 (*Sir F.H. Hinsley*, et al., British Intelligence in the Second World War, Vol. II, 56).

[61] *Christopher Andrew*, The making of the Anglo-American SIGINT Alliance, ibidem, 101 (*Sir F.H. Hinsley*, et al., British Intelligence in the Second World War, Vol. II, 48).

[62] *Christopher Andrew*, The making of the Anglo-American SIGINT Alliance, ibidem, 101f: Interviews mit

Après la guerre, c'est surtout la Grande-Bretagne qui préconisa le maintien d'une alliance SIGINT. Les bases en furent convenues lors d'une tournée mondiale effectuée, au printemps 1945, par des agents de renseignement britanniques (parmi lesquels Sir Harry Hinsley, dont les livres sont à la base de l'article cité). Un des objectifs était d'envoyer du personnel SIGINT d'Europe dans le Pacifique, dans le cadre de la guerre contre le Japon. Dans ce contexte, il fut convenu avec l'Australie de mettre des ressources et du personnel (britannique) à la disposition des services australiens. Le voyage de retour, via la Nouvelle-Zélande et le Canada, conduisait aux États-Unis.

En septembre 1945, Truman signa un mémorandum top secret qui constituait la clef de voûte d'une alliance SIGINT en temps de paix[63]. Puis Britanniques et Américains ouvrirent des négociations en vue de la conclusion d'un accord. De plus, une délégation britannique prit contact avec les Canadiens et les Australiens, pour discuter d'une participation éventuelle. En février et mars 1946, une conférence SIGINT anglo-américaine se tint dans le plus grand secret, pour discuter des détails. Les Britanniques étaient mandatés par les Canadiens et les Australiens. La conférence aboutit à un accord de quelque 25 pages, toujours classifié, qui arrêtait les détails d'un accord SIGINT entre les États-Unis et le Commonwealth britannique. D'autres négociations eurent lieu au cours des deux années suivantes, de sorte que le texte final de l'accord dit UKUSA put être signé en juin 1948[64].

5.4.2. Éléments attestant l'existence de l'accord

5.4.2.1. Rapport annuel 1999/2000 de la commission britannique du renseignement et de la sécurité

Pendant longtemps, les États signataires n'ont jamais reconnu officiellement l'existence de l'accord UKUSA. Dans le rapport annuel de la commission du renseignement et de la sécurité, organe de contrôle parlementaire au Royaume-Uni, l'accord UKUSA est mentionné explicitement.[65]

Sir F.H. Hinsley, "Operations of the Military Intelligence Service War Department London (MIS WD London)" 11 June 1945, Tab A, RG 457 SRH-110, NAW.

63 *Harry S. Truman*, Memorandum for the Secretaries of the State, War and the Navy, 12 Sept. 1945: „The Secretary of War and the Secretary of the Navy are hereby authorised to direct the Chief of Staff, U.S. Army and the Commander in Chief, U.S. Fleet; and Chief of Naval Operations to continue collaboration in the field of communication intelligence between the United States Army and Navy and the British, and to extend, modify or discontinue this collaboration, as determined to be in the best interests of the United States.“ (cité par *Bradley F. Smith*, The Ultra-Magic Deals and the Most Secret Special Relationship (Presidio 1993)).

64 *Christopher Andrew*, “The making of the Anglo-American SIGINT Alliance” in *Hayden*, *Peake* and *Samuel Halpern* eds, In the Name of Inteligence. Essays in Honor of *Walter Pforzheimer*, (NIBC Press 1995), 95 – 109: Interviews with Sir Harry Hinsley, March/April 1994, who did a part of the negotiations; Interviews with Dr. Louis Tordella, Deputy Director of NSA from 1958 to 1974, who was present at the signing.

65 Intelligence and Security Committee Annual Report 1999-2000. Presented to Parliament by the Prime Minister by Command of Her Majesty, November 2000, 8 Rz 14.
Texte original: "The quality of intelligence gathered clearly reflects the value of the close co-operation under the UKUSA agreement. A recent illustration of this occurred when the US National Security Agency's (NSA) equipment accidentally failed and for some three days US customers, as welle as GCHQ's normal UK customers, were served directly from GCHQ.".

5.4.2.2. Informations fournies par les services du Premier Ministre de Nouvelle-Zélande

Des informations publiées l'an dernier par les services du Premier ministre de Nouvelle-Zélande au sujet des services nationaux de sécurité et de renseignements en font mention explicitement.[66] D'autres éléments attestent clairement son existence.

5.4.2.3. Liste des acronymes utilisés par la Navy

Selon la marine américaine[67], UKUSA veut dire "United Kingdom, USA" et désigne "un accord SIGINT entre cinq nations".

5.4.2.4. Déclaration du directeur du DSD

Lors d'une interview, le directeur du service de renseignements australien (DSD) a confirmé l'existence de cet accord: selon lui, les services secrets australiens coopèrent avec d'autres services de renseignements d'outre-mer dans le cadre de l'accord UKUSA[68].

5.4.2.5. Rapport du Canadian Parliamentary Security and Intelligence Committee

Ce rapport indique que le Canada coopère, en matière de renseignements, avec certains de ses alliés les plus anciens et les plus proches. Il nomme ces alliés: les États-Unis (NSA), le Royaume-Uni (GCHQ), l'Australie (DSD) et la Nouvelle-Zélande (GCSB). Il ne donne pas la dénomination de l'accord.

5.4.2.6 Déclaration de M. Louis Torella, ancien directeur adjoint de la NSA

Dans une interview donnée, en novembre 1987 et avril 1992, à Christopher Andrew, professeur à l'Université de Cambridge, M. Louis Torella, qui était présent lors de la signature, confirme l'existence de l'accord[69].

---

66 Domestic and External Secretariat du Department of the Prime Minister and Cabinet de Nouvelle Zélande, Securing our Nation's Safety. How New Zealand manages its security and intelligence agencies (2000). Texte original: "The operation of the GCSB is directed solely by the New Zealand Government. It is, however, a member of a long-standing collaborative international partnership for the exchange of foreign intelligence and the sharing of communications security technology. The other members of the partnership are the USA's National Security Agency (NSA), the UK's Government Communications Headquarters (GCHQ), Australia's Defence Signals Directorate (DSD) and Canada's Communications Security Establishment (CSE). New Zealand gains considerable benefit from this arrangement, as it would be impossible for New Zealand to generate the effectiveness of the five nation partnership on its own.".

67 „Terms/Abbreviations/Acronyms“ veröffentlicht durch das US Nave and Marine Corps Intelligence Training Centre (NMITC) bei http://www.cnet.navy.mil/nmitc/training/u.html.

68 *Martin Brady*, Direktor des DSD, Lettre du 16.3.1999 à Ross Coulthart, Sunday Program Channel 9.

69 *Andrew, Christopher* "The growth of the Australian Intelligence Community and the Anglo-American Connection", 223-4.

5.4.2.7 Lettre de M. Joe Hooper, ancien directeur du GCHQ

Dans une lettre au Marshall S. Carter, ancien directeur de la NSA, M. Joe Hooper, ancien directeur du GCHQ, confirme l'existence de l'accord UKUSA.

5.4.2.8 Interlocuteurs du rapporteur

Le rapporteur a discuté de l'accord UKUSA avec plusieurs personnes qui, de par leurs fonctions, doivent connaître cet accord et son contenu. Dans tous les cas, le style des propos tenus a confirmé indirectement l'existence de cet accord.

5.5. Exploitation des documents américains ayant cessé d'être classés confidentiels

5.5.1. Nature des documents

Dans le cadre du "Freedom of Information Acts" de 1966 (5 U.S.C. § 552) et du règlement du ministère de la défense (DoD FOIA règlement 5400.7-R de 1997), des documents classés précédemment secrets ont cessé de l'être et sont ainsi devenus accessibles à tous.

Le public peut avoir accès aux documents par l'intermédiaire de la National Security Archive créée en 1985 (George Washington University, Washington D.C.). Jeffrey Richelson, ancien membre de la National Security Archive, a communiqué par internet 16 documents, qui donnent une idée de la genèse, du développement, de la gestion et du mandat de la NSA (National Security Agency)[70]. De plus, deux des documents citent le nom d'ECHELON. Ces documents sont sans cesse mentionnés par différents auteurs ayant écrit à propos d'ECHELON, qui les considèrent comme la preuve de l'existence du système d'espionnage mondial ECHELON. En outre, certains des documents mis à disposition par Richelson, confirment l'existence du NRO (National Reconnaissance Office) et constatent que sa mission consiste à gérer et à exploiter les satellites SIGINT[71]. Comme suite à l'entretien avec Jeffrey Richelson à Washington, ce dernier a transmis à la commission d'autres documents qui ne sont plus couverts par le secret. Il a été tenu compte de ceux qui étaient intéressants du point de vue de l'enquête.

5.5.2. Contenu des documents

Dans ces documents, on peut trouver des descriptions ou mentions fragmentaires des thèmes suivants:

[70] *Richelson, Jeffrey T.*, The National Security Agency Declassified, National Security Archive Electronic Briefing Book n°. 24, George Washington University http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB23/index.html.

[71] *Richelson, Jeffrey T.*, The National Security Agency Declassified, National Security Archive Electronic Briefing Book n°. 24, George Washington University http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB35/index.html.

5.5.2.1. Mission et conception de la NSA (documents 1, 2b, 4, 10 et 16)

Dans la directive 9 du National Security Council Intelligence (NSCID 9) du 10 mars 1950[72], la notion de communication extérieure est définie au sens du COMINT; c'est ainsi qu'il faut entendre par **communication extérieure toute communication gouvernementale au sens large (pas uniquement militaire), ainsi que toute autre communication, pouvant contenir des informations d'intérêt militaire, politique, scientifique ou économique**.

La directive (NSCID 9 rév. du 29.12.1952)[73] stipule que le FBI est seul responsable pour la sécurité intérieure.

La directive du ministère de la défense du 23 décembre 1971[74] (DoD) concernant la NSA et le Central Security Service (CSS) définit comme suit ce concept pour la NSA:

– la NSA est un service distinct au sein du ministère de la défense, qui est placé sous la direction du ministère de la défense;

– la NSA assure, d'une part, la mission SIGINT des États-Unis et met, d'autre part, à la disposition de tous les ministères et services des systèmes de communication sûrs;

– l'activité SIGINT de la NSA ne s'étend pas à la production et à la diffusion d'informations déjà traitées. Cette tâche est du ressort d'autres ministères et services.

Par ailleurs, la directive DoD de 1991 présente, dans les grandes lignes, la structure de la NSA et du CSS.

Dans une déclaration qu'il a faite le 12 avril 2000[75] devant la commission d'enquête permanente "Renseignement" de la chambre des représentants, Hayden, directeur de la NSA, décrit comme suit les missions de la NSA:

– la surveillance électronique sert à rassembler des communications extérieures à l'intention des militaires et responsables politiques (décideurs politiques);

– la NSA fournit aux consommateurs gouvernementaux américains des renseignements sur le terrorisme international, la drogue, la prolifération des armements;

– la NSA n'a pas pour mission de collecter toutes les communications électroniques;

– la NSA ne peut transmettre des informations qu'à des destinataires autorisés par le gouvernement; elle ne peut en transmettre directement aux entreprises américaines.

---

[72] Document 1. NSCID 9, "Communications Intelligence," March 10, 1950.
[73] Document 2b. National Security Council Intelligence Directive n° 9, Communication Intelligence, December 29, 1952.
[74] Document 4. Department of Defense Directive S-5100.20, "The National Security Agency and the Central Security Service," December 23, 1971.
[75] Document 16. Statement for the Record of NSA Director Lt Gen Michael V. Hayden, USAF before the House Permanent Selct Committee on Intelligence, April 12,2000.

Dans un mémorandum du vice-amiral des forces navales américaines, W.O. Studeman, établi au nom du gouvernement, en date du 8 avril 1992[76], il est fait état du caractère de plus en plus mondial (access) de la mission de la NSA, parallèlement au "Support of military operations".

5.5.2.2. Pouvoirs des services de renseignement (document 7)[77]

Il ressort de la directive 18 de l'United States Signals Intelligence (USSID 18) que les signaux acheminés par câble comme les signaux hertziens sont interceptés.

5.5.2.3. Coopération avec d'autres services (documents 2 a et 2 b)

Au nombre des tâches incombant au Communications Intelligence Board américain, il y a notamment la surveillance de tous les "arrangements" avec les gouvernements étrangers dans le domaine COMINT. Le directeur de la NSA est entre autres responsable de tous les contacts avec les services COMINT étrangers.[78]

5.5.2.4. Mention des unités actives sur les "sites ECHELON" (documents 9 et 12)

Dans les instructions C5450.48A[79] du NAVSECGRU, le mandat, la fonction et l'objectif de la Naval Security Group Activity (NAVSECGRUACT), 544e Intelligence Group de Sugar Grove, Virginie occidentale, sont décrits. Il y est indiqué qu'une mission spécifique consiste à gérer et exploiter un site ECHELON; une autre mission citée est le traitement des informations provenant des services de renseignement.

Dans le document "History of the Air Intelligence Agency – 1 January to 31 December 1994"[80], il est fait mention au point "Activation of Echelon Units" de l'Air Intelligence Agency (AIA), detachment 2 et 3:

Les documents ne disent nullement en quoi consiste un "site ECHELON", ce qui est fait sur un "site ECHELON", ni ce que recouvre l'appellation ECHELON. De même, les documents ne permettent pas de savoir en quoi consiste l'accord UKUSA.

5.5.2.5. Mention de stations (documents 6, 9 et 12, nouveaux documents)

– Sugar Grove (Virginie occidentale), cité comme Station SIGINT dans les NAVSECGRU INSTRUCTIONS C5450.48A,[81]

---

[76] Document 10. Farewell from Vice Admiral William O. Studeman to NSA Employees, April 8, 1992.

[77] Document 7. United States Signals Intelligence Directive [USSID] 18, "Legal Compliance and Minimization Procedures", JUly 27, 1993.

[78] Document 2a. Memorandum from President Harry S. Truman to the Secretary of State, the Secretary of Defense, Subject: Communications Intelligence Activities, October 24, 1952.

[79] Document 9. navsecgru Instruction C5450.48A, Subj.:Mission, Functions and Tasks of Naval Security Group Activity (NAVSECGRUACT) Sugar Grove, West Virginia, September 3, 1991.

[80] Document 12. "Activation of Echelon Units", from History of the Air Intelligence Agency, 1 January – 31 December 1994, Volume I (San Antonio, TX: AIA, 1995.

[81] Document 9. NAVSECGRU Instruction C5450.48A, Subj: Mission, Functions and Tasks of Naval Security Group Activity (NAVSECGRUACT) Sugar Grove, West Virginia, September 3, 1991.

– Misawa Air Base (Japon), cité comme station SIGINT dans History of the Air Intelligence Agency – January to 31 December 1994[82],et dans la description des activités du Naval Security Group dans les documents du ministère de la Marine[83]

– Porto Rico (Sabana Seca),cité comme station SIGINT dans History of the Air Intelligence Agency – January to 31 December 1994, et dans la description des activités du Naval Security Group dans les documents du ministère de la Marine[84]

– Guam, cité comme station SIGINT, ibidem

– Yakima (Washington), cité comme station SIGINT, ibidem

– Fort Meade (Maryland); un rapport COMINT de la NSA émanant de Fort George G. Meade (Maryland), en date du 31 août 1972, prouve l'existence d'activités COMINT en cet endroit.[85]

– Menwith-Hill, Royaume-Uni, description des activités du Naval Security Group dans les documents du ministère de la marine[86]

– Bad Aibling, Allemagne, description des activités du Naval Security Group dans les documents du ministère de la marine[87]

– Medina, Texas, description des activités du Naval Security Group dans les documents du ministère de la marine[88]

– Kunia, Hawaii, description des activités du Naval Security Group dans les documents du ministère de la marine[89]

5.5.2.6. Protection de la vie privée des citoyens américains (documents 7, 7a à f, 9, 11 et 16)

Les NAVSECGRU INTRUCTIONS C5450.48A arrêtent qu'il faut protéger la vie privée des citoyens.[90]

---

[82] Document 12. "Activation of Echelon Units, "from History of the Air Intelligence Agency, 1 January – 31 December 1994, Volume I (San Antonio, TX: AIA, 1995).

[83] Department of the Navy, Naval Security Group Instruction C5450.32E du 9.5.1996.

[84] Naval Security Group Instruction C5450.33B du 8.8.1996.

[85] COMINT Report de la NSA de Fort George G. Meade, Maryland du 31 août 1972.

[86] Department of the Navy, Fact and Justification Sheet for the Establishment of U.S. Naval Security Group Activity.

[87] Department of the Navy, Naval Security Group Instruction C55450.63 du 25.10.1995.

[88] Department of the Navy, Naval Security Group Instruction C5450.60A du 8.4.1996

[89] Naval Security Group Instruction C5450.55B du 8.8.1996

[90] Document 9. NAVSECGRU Instruction C5450.48A, Subj: Mission, Functions and Tasks of Naval Security Group Activity (NAVSECGRUACT) Sugar Grove, West Virginia, September 3, 1991

Différents documents expliquent que la vie privée des citoyens américains doit être protégée, indiquant comment le faire (Baker, General Counsel, NSA, lettre du 9 septembre 1992, United States Signals Intelligence Directive (USSID) 18, 20 octobre 1980, et différents suppléments[91].

5.5.2.7. Définitions (documents 4, 5a et 7)

La directive du ministère de la défense du 23 décembre 1991[92] donne des définitions précises de SIGINT, COMINT, ELINT et TELINT, tout comme la directive n° 6 du National Security Council Intelligence du 17 février 1972.[93]

Selon ces définitions, il faut entendre par COMINT la collecte et le traitement des communications extérieures (acheminées par des moyens électromagnétiques), ainsi que l'interception et le traitement des communications écrites non cryptées, de la presse et de la propagande, à moins qu'elle ne soit cryptée.

5.5.3. Résumé

1. Voici 50 ans déjà, les informations jugées intéressantes concernaient les domaines non seulement de la politique et de la sécurité mais aussi de la science et de l'économie.

2. Les documents prouvent que la NSA collabore avec d'autres services dans le domaine COMINT.

3. Les documents qui fournissent des renseignements sur l'organisation de la NSA, les missions de celle-ci et ses liens avec le ministère de la défense n'apportent pas véritablement de renseignements supplémentaires par rapport aux sources publiquement accessibles de la page d'accueil de la NSA.

4. Les communications par câble peuvent être interceptées.

5. Le 544e Intelligence groupe et les Detachments 2 et 3 de l'Air Intelligence Agency participent à la collecte des informations du renseignement.

6. Le nom d'"ECHELON" apparaît dans différents contextes.

7. S'agissant des stations SIGINT, les noms suivants sont cités: Sugar Grove (Virginie occidentale), Misawa Air Base (Japon), Porto Rico (Sabana Seca), Guam, Yakima (État

---

[91] Dissemination of U.S. Government Organizations and Officials, Memorandum du 5 février 1993; Reporting Guidance on References to the First Lady, 8 juillet 1993; Reporting Guidance on Former President Carter's Involvement in the Bosnian Peace Process, 15 décembre 1994; Understanding USSID 18, 30 septembre 1997; USSID 18 Guide, 14 février 1998;
NSA/US IDENTITIES IN SIGINT, mars 1994; Statement for the record of NSA Director Lt Gen. *Michael V. Hayden*, USAF, 12 avril 2000).

[92] Document 4. Department of Defense Directive S-5100.20, "The National Security Agency and the Central Security Service," December 23, 1971

[93] Document 5a. NSCID 6, "Signals Intelligence," February 17, 1972.

de Washington).

8. D'autres stations où opère le Naval Security Group sont citées mais non décrites comme stations SIGINT.

9. Les documents indiquent comment la vie privée des citoyens américains doit être protégée.

S'ils n'apportent aucune preuve concrète, les documents n'en fournissent pas moins de véritables indices, qui conjointement avec d'autres, permettent de tirer des conclusions.

5.6. RENSEIGNEMENTS ÉMANANT D'AUTEURS SPÉCIALISÉS ET DE JOURNALISTES

5.6.1. Nicky Hager

Dans le livre de l'auteur néo-zélandais, Nicky Hager, "Secret Powers – New Zealand's role in the international spy network" paru en 1996, le système ECHELON est décrit pour la première fois dans le détail. Il se base sur des entretiens avec plus de 50 personnes employées par le service de renseignements néozélandais ou engagées par ailleurs dans des activités de renseignement. De plus, il a analysé de nombreux documents provenant des archives nationales de journaux et d'autres sources publiques. D'après Hager, le système est dénommé ECHELON et les ordinateurs du réseau sont dénommés "dictionnaires ECHELON".

Selon l'auteur, l'origine du système ECHELON remonte à 1947, année où, dans le prolongement de la coopération de l'époque de guerre, le Royaume-Uni et les États-Unis sont convenus de poursuivre à l'échelle mondiale pour ainsi dire les activités de "renseignement transmissions" (COMINT). Ces deux pays devaient collaborer pour mettre en place un système d'interception autant que possible mondial, étant entendu qu'ils se partageraient les équipements spécifiques nécessaires à cet effet, ainsi que les dépenses occasionnées, et qu'ils auraient l'un et l'autre accès aux résultats. Par la suite, le Canada, l'Australie et la Nouvelle-Zélande ont adhéré au pacte UKUSA.

Selon Hager, l'interception des communications satellitaires constitue l'élément central du système actuel. Dès les années 70, les communications acheminées par Intelsat – le premier système mondial de télécommunications par satellites[94] – furent interceptées par des stations au sol. Ces informations étaient alors étudiées aux moyens d'ordinateurs sur la base de mots-clés ou d'adresses préprogrammés en sorte de filtrer les informations importantes. Par la suite, la surveillance a été étendue à d'autres satellites, comme par exemple ceux d'Inmarsat[95], organisation dont les activités concernent principalement les communications maritimes.

[94] Cf.: http://www.intelsat.int/index.htm.
[95] Cf.: http://www.inmarsat.org/index3.html.

Hager signale dans son livre que l'interception des communications satellitaires ne constitue qu'une composante – certes importante – du système d'interception géant. Parallèlement, il existerait de nombreuses autres installations de surveillance du faisceau hertzien et des câbles, à propos desquelles les documents sont toutefois moins nombreux et dont il est difficile de prouver l'existence, dès lors que contrairement aux stations au sol, elles peuvent pratiquement passer inaperçues. Echelon est ainsi devenu le synonyme d'un système d'interception mondial.

Dans l'exposé qu'il a fait le 24 avril 2001 devant la commission, Hager a souligné que le système d'interception n'était pas tout-puissant. Étant donné qu'il faut utiliser au mieux les ressources limitées, tout ne peut pas être intercepté: il faut se contenter de ce qui promet des informations importantes. Les objectifs sont donc en général constitués par des informations politiques et diplomatiques. Si l'interception a pour objectif d'obtenir des informations écnomiques, celles-ci s'inscrivent plutôt dans un contexte macroéconomique que microéconomique.

S'agissant des méthodes de travail du système, chaque partenaire a ses propres listes de mots-cibles. En outre, les communications sont également analysées sur la base de mots-clés injectés dans le système par les États-Unis au moyen de "dictionary managers". Les Britanniques n'ont aucun contrôle sur cet aspect et ignorent quelles informations sont collectées à Morwenstow parce que celles-ci sont directement transmises aux États-Unis.

Dans ce contexte, Hager a souligné le risque que peuvent constituer les stations d'interception britanniques pour l'Europe continentale. Citant de nombreux exemples, il a fait observer que les partenaires UKUSA du Pacifique espionnaient leurs alliés et leurs partenaires commerciaux. Les seules personnes qui échappaient à l'espionnage étaient les partenaires UKUSA. Il a estimé que les services secrets britanniques et les Néozélandais seraient sans doute très réticents à compromettre le partenariat UKUSA en refusant de coopérer et d'écouter l'Europe continentale. Rien n'inciterait le Royaume-Uni à renoncer à des informations intéressantes et, étant donné qu'elles sont toujours secrètes, l'espionnage pratiqué dans le cadre de l'accord UKUSA n'exclurait pas une politique officielle de loyauté vis-à-vis de l'Europe.

5.6.2. Duncan Campbell

Le journaliste britannique Duncan Campbell s'appuie dans ses nombreuses publications sur les travaux de Hager et Richelson ainsi que sur des entretiens avec d'anciens collaborateurs des services secrets, de même que sur d'autres recherches. Selon lui, ECHELON fait partie du système mondial qui intercepte et analyse les communications internationales par satellite. Chaque État membre dispose d'ordinateurs "Dictionary" qui analysent les communications interceptées à partir de mots-clés.

Dans l'étude 2/5 de 1999 du STOA qui examine de façon approfondie les aspects techniques, dont il a été question précédemment, Duncan Campbell démontrait dans le détail – en expliquant comment – que chaque moyen utilisé aux fins de communication pouvait être intercepté. Dans une de ses dernières études, il constatait toutefois clairement qu'ECHELON avait lui aussi ses limites, et que l'idée selon laquelle une surveillance sans faille était possible s'était révélée infondée, soulignant qu'ECHELON et le système d'espionnage électronique dont il forme une partie ne sont pas en mesure d'assurer une telle surveillance, et qu'en outre, l'équipement qui permettrait de traiter et de reconnaître la nature de toute communication orale ou de tout appel

téléphonique n'existait pas[96].

Dans l'exposé qu'il a fait devant la commission le 22 janvier 2001, Campbell a estimé que les USA faisaient appel à leurs services de renseignements pour aider les entreprises américaines à obtenir des marchés. Les informations intéressantes sont transmises aux entreprises via la CIA, avec l'aide de l'Advocacy Center et de l'Office of Executive Support au Department of Commerce. À l'appui de cette hypothèse, il a présenté des documents desquels il ressort que l'Advocacy Center est intervenu à l'avantage d'entreprises américaines. L'information figure aussi largement sur la page d'accueil de l'Advocacy Center.[97] Dire que la réussite de l'Advocacy Center s'explique par les écoutes relève de la spéculation et cela ne ressort pas des documents.

Campbell a souligné au cours de son exposé que les capacités d'interception de plusieurs pays européens s'étaient nettement accrues au cours des dernières années – notamment en Suisse, au Danemark et en France. On observe par ailleurs un renforcement de la coopération bilatérale et multilatérale dans le domaine du renseignement.

5.6.3. Jeff Richelson

Jeff Richelson, auteur américain et ancien membre des National Security Archives, a fourni par internet l'accès à seize documents précédemment secrets qui donnent un aperçu de la genèse, du développement, de la gestion et du mandat de la NSA (National Security Agency)[98].

Il est en outre l'auteur de différents ouvrages et articles sur les activités des services de renseignements des États-Unis. Ses travaux s'appuient sur de nombreux documents ayant cessé d'être secrets, sur le travail de recherche de Hager ainsi que sur ses recherches personnelles. Lors de sa rencontre avec la délégation de la commission à Washington DC, le 11 mai 2001, il a déclaré qu'ECHELON désignait un réseau d'ordinateurs, au moyen duquel seraient filtrées des données échangées entre les services de renseignements.

Dans son livre intitulé "The ties that binds"[99], publié en 1985, il décrit dans le détail la genèse de l'accord UKUSA et les activités menées dans ce contexte par les services secrets participants des États-Unis, du Royaume-Uni, du Canada, d'Australie et de Nouvelle-Zélande.

Dans son volumineux ouvrage intitulé "The U.S Intelligence Community"[100], de 1999, il donne un aperçu des activités des services secrets des États-Unis et décrit les structures d'organisation des services ainsi que leurs méthodes de collecte et d'analyse du renseignement. Au chapitre 8 de cet ouvrage, il fournit des détails sur les capacités SIGINT des services et décrit quelques stations au sol. Au chapitre 13, il dépeint les relations des États-Unis avec d'autres services de renseignements, notamment l'accord UKUSA.

---

[96] *Duncan Campbell*, Inside Echelon. The history, structure and function of the global surveillance system knows as Echelon, http://www.heise.de/tp/deutsch/special/ech/6928/l.html

[97] Homepage des Advocay Centers, http://www.ita.doc.gov/td/advocacy/index.html
Le rapporteur a souhaité permettre à l'Advocacy Center de prendre position sur ces allégations lors de sa mission à Washington DC. Le Commerce Department Center a cependant annulé le rendez-vous.

[98] Jeffrey T. Richelson, The National Security Agency Declassified, National Security Archive Electronic Briefing Book no. 24, George Washington University, http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB23/index.html

[99] Jeffrey T. Richelson, Desmond Ball, The Ties That Bind, Boston UNWIN HYMAN (1985).

[100] Jeffrey T. Richelson, The U.S. Intelligence Community, Westview Press (1999).

Dans un article intitulé "Desperately seeking Signals"[101], publié en 2000, il expose brièvement le contenu de l'accord UKUSA, cite des installations d'interception de communications par satellites et renseigne les possibilités et les limites de l'interception de communications civiles.

5.6.4. James Bamford

L'auteur américain James Bamford, qui fonde également ses travaux sur des recherches dans les archives ainsi que sur l'interrogatoire de collaborateurs des services de renseignement, fut le premier à s'intéresser à l'activité SIGINT de la NSA. En 1982 déjà, il publiait "The Puzzle palace" [102], décrivant dans le détail, en son chapitre 8 "Partners", l'accord UKUSA. Selon son nouveau livre "Body of Secrets"[103], qui fait fond sur les faits révélés dans "The Puzzle Palace", le réseau informatique qui relie les services de renseignement s'appelle "Plattform", ECHELON désignant pour sa part le logiciel, utilisé dans toutes les stations, qui permet un traitement unique et un accès direct aux données[104]. Dans les chapitres qui suivent, il emploie toutefois également le nom ECHELON pour désigner le système d'interception dans le cadre de l'accord UKUSA.

Dans "Body of Secrets" – et ce en son chapitre "Muscle" tout particulièrement intéressant en l'occurrence –, Bamford brosse l'histoire du développement de la surveillance des communications par la NSA et décrit la capacité du système, le fonctionnement du partenariat UKUSA et les objectifs de celui-ci. Il souligne que les interviews de dizaines d'agents actuels et anciens de la NSA démontrent que celle-ci n'est pas impliquée dans l'espionnage de concurrence.

Ce dire, il l'a confirmé lors de son audition devant la commission ECHELON le 23 avril dernier. L'utilisation de la NSA aux fins de l'espionnage de concurrence nécessiterait une décision politique claire au plus haut niveau politique, décision qui n'a toujours pas été prise jusqu'ici. Au cours de ses vingt années de recherche, il n'a jamais eu la preuve que la NSA transmettait à des entreprises américaines des informations obtenues par les services de renseignement, y compris dans le cas, par exemple, où elle intercepte les communications d'entreprises privées pour s'assurer du respect d'embargos.

Selon les déclarations de Bamford, le problème majeur pour l'Europe résiderait dans la question de savoir non pas si le système ECHELON vole des secrets d'entreprises et les communique à leurs concurrents mais bien s'il y a violation du droit fondamental à la vie privée. Dans "Body of Secrets", il décrit de façon détaillée comment la protection des "US persons" (c'est-à-dire les citoyens américains et les personnes résidant légalement aux États-Unis) s'est développée, faisant observer qu'il existe également pour d'autres résidents UKUSA à tout le moins des restrictions internes. Parallèlement, il signale qu'il n'existe pas de protection pour d'autres personnes ni d'obligation d'élimination des données, et que les capacités de mémorisation de la NSA sont pour ainsi dire incommensurables.

---

[101] *Jeffrey T. Richelson*, Desperately seeking Signals,The Bulletin of the Atomic Scientists, Vol. 56, No. 2/2000, 47-51, http://www.bullatomsci.org/issues/2000/ma00/ma00richelson.html

[102] *James Bamford,* The Puzzle Palace, Inside the National Security Agency, America's most secret intelligence organization (1983).

[103] *James Bamford,* Body of Secrets. Anatomy of the Ultra-Secret National Security Agency. From the Cold War Through the Dawn of a New Century, Doubleday Books (2001).

[104] *James Bamford,* Body of Secrets. Anatomy of the Ultra-Secret National Security Agency. From the Cold War Through the Dawn of a New Century, Doubleday Books (2001), 404.

Néanmoins, Bamford met aussi l'accent sur les limites du système qui procèdent du fait, d'une part, qu'une petite partie seulement des communications internationales est effectuée par satellite et qu'il est beaucoup plus difficile d'intercepter les communications par câbles à fibres optiques, et, d'autre part, que la NSA ne dispose que de capacités limitées d'exploitation finale, alors que le flux des communications, en particulier via le réseau internet, ne cesse de croître.

5.6.5. Bo Elkjaer et de Kenan Seeberg

Les deux journalistes danois Bo Elkjaer et Kenan Seeberg ont déclaré, le 22 janvier 2001 devant la commission, qu'ECHELON avait déjà atteint un stade très avancé dans les années 80. Le Danemark , qui avait nettement renforcé ses capacités d'interception au cours de la dernière décennie, collabore avec les États-Unis depuis 1984.

Dans un article paru dans Ekstra Bladet[105], où ils se référaient à la présentation de diapositives (25 diapositives) par un officier non nommé du 544e Intelligence Group de l'Air Intelligence Agency, ils signalaient que différentes ONG (au nombre desquelles la Croix-Rouge) étaient la cible de l'activité d'ECHELON.

5.7. Déclarations d'anciens collaborateurs des services de renseignements

5.7.1. Margaret Newsham (ex-collaboratrice de la NSA)[106]

Margaret Newsham a été employée, de 1974 à 1984, par Ford et Lockheed, et elle a travaillé pendant ce temps, selon ses propres dires, pour la NSA. Elle a été formée pour son travail au quartier général de la NSA à Fort George Meade (Maryland, États-Unis), et a travaillé de 1977 à 1981 à Menwith Hill, la station terrestre américaine en territoire britannique. Là, elle a eu l'occasion d'écouter une conversation du sénateur américain Strohm Thurmond au sénat. Dès 1978, ECHELON pouvait intercepter les télécommunications d'une personne donnée effectuées par satellite.

S'agissant de son propre rôle au sein de la NSA, elle aurait eu la responsabilité d'élaborer des systèmes et programmes, de les configurer et de les rendre opérationnels sur de grands ordinateurs. Les logiciels s'appelaient SILKWORTH et SIRE, ECHELON étant le nom du réseau.

---

[105] *Bo Elkjaer, Kenan Seeberg,* ECHELON singles out the Red Cross, A bombshell in the surveillance scandal: The organization is a possible surveillance target, Ekstra Bladet, Danemark, 8.3.2000, http://cryptome.org/echelon-red.htm

[106] *Bo Elkjaer, Kenan Seeberg*, Echelon was my baby – Interview with Margaret Newsham, Ekstra Bladet, 17.1.1999.

5.7.2. Wayne Madsen (ancien collaborateur de la NSA)

Wayne Madsen[107], ancien collaborateur de la NSA, confirme également l'existence d'ECHELON. Selon lui, la collecte des données économique se voit reconnaître un caractère véritablement prioritaire et son objet consiste à procurer des avangages aux entreprises américaines. Il craint en particulier qu'ECHELON ait pu espionner des ONG comme Amnesty International ou Greenpeace. Il déclare également que la NSA a dû admettre qu'elle disposait de plus de mille pages d'informations sur la princesse Diana, dont la campagne contre les mines terrestres dérangeait la politique américaine.

Lors de sa rencontre avec la délégation de la commission à Washington DC, il s'est dit particulièrement préoccupé par le danger que représentait le système d'espionnage mondial pour la vie privée des citoyens européens.

5.7.3. Mike Frost (ancien collaborateur des services secrets canadiens)

Mike Frost a travaillé pendant plus de vingt ans dans le service secret canadien CSE[108]. La station d'interception d'Ottawa ne serait qu'un élément d'un réseau mondial de stations d'espionnage[109]. Dans une interview accordée à la CBS, il a déclaré que partout dans le monde, chaque jour, les communications téléphoniques, les courriers électroniques et les fax étaient surveillés par ECHELON, qui était un réseau de surveillance secret du gouvernement[110]. Il en allait également ainsi pour les communications civiles. À titre d'exemple, il cite dans une interview accordée à une radio australienne, un cas dans lequel le CSE avait effectivement enregistré le nom et le numéro de téléphone d'une femme dans une base de données concernant des terroristes éventuels, cette femme ayant employé une notion ambigüe dans une conversation téléphonique innocente avec un ami. En filtrant les communications, l'ordinateur avait rencontré le mot-clé et retransmis la communication, le responsable de l'analyse qui ne savait pas réellement que penser, ayant ainsi enregistré ses données personnelles[111].

Les services de renseignement des pays UKUSA s'aideraient également mutuellement, en ce sens qu'un service espionnerait pour le compte d'un autre, en sorte que rien ne pourrait être reproché au service de renseignement local du moins. Ainsi, le GCHQ britannique aurait demandé au CSE canadien d'espionner pour son compte deux ministres anglais, le premier ministre, Mme Thatcher, voulant savoir si ceux-ci se rangeaient à ses côtés[112].

---

[107] Interview de NBC "60 Minutes" du 27.2.2000; http://cryptome.org/echelon-60min.htm.
[108] Communication Security Establishment, service dépendant du ministère canadien de la défense, qui est chargé de l'activité Sigint.
[109] Interview de NBC "60 Minutes" du 27.2.2000; http://cryptome.org/echelon-60min.htm.
[110] *Florian Rötzer*, Die NSA geht wegen Echelon an die Öffentlichkeit; http://www.heise.de/bin/tp/issue/download.cgi?artikelnr=6633&rub_ordner=special.
[111] Interview de NBC "60 Minutes" du 27.2.2000; http://cryptome.org/echelon-60min.htm.
[112] Interview de la chaîne australienne Channel 9 du 23.3.1999; http://www.geocities.com/CapitolHill/Senate/8789/sunday1.htm.

5.7.4. Fred Stock (ancien collaborateur des services secrets canadiens)

Selon ses propres dires, Fred Stock a été exclu du service secret canadien CSE en 1993, parce qu'il avait protesté contre la nouvelle orientation du service qui mettait davantage l'accent sur des informations économiques et des objectifs civils. Les communications interceptées auraient fourni des informations sur des opérations commerciales avec d'autres pays, notamment les négociations sur l'ALENA, l'achat de céréales par la Chine, et les ventes d'armes françaises. Selon Stock, le service se serait également procuré de façon habituelle des informations sur des actions environnementales menées par des navires de Greenpeace en haute mer[113].

5.8. Informations de sources gouvernementales

5.8.1. Déclarations américaines

James Woolsey, ancien directeur de la CIA, a déclaré à l'occasion d'une conférence de presse[114], donnée à la demande du ministère américain des affaires étrangères, que les États-Unis se livraient à des activités d'espionnage en Europe continentale. Le renseignement économique proviendrait toutefois à hauteur de 95 % de l'exploitation des sources d'information publiques, les secrets volés ne représentant que 5 %. Les données économiques d'autres pays sont espionnées dans des cas en rapport avec le respect de sanctions et les biens à double usage, ainsi que les tentatives de corruption lors de la passation de marchés. Ces informations ne sont toutefois pas communiquées aux entreprises américaines. Woolsey a souligné que même lorsque l'activité d'espionnage des données économiques permet de découvrir des informations dont l'utilisation présenterait un intérêt économique, il faudrait beaucoup de temps à un analyste pour exploiter la quantité importante de données existant dans ce domaine et qu'il serait irrationnel de perdre son temps à espionner des partenaires commerciaux amis. De plus, il a fait observer que même si cela était fait, il serait difficile, compte tenu des interdépendances internationales, de savoir quelle entreprise doit être réputée américaine et se voir confier ainsi les informations obtenues.

[113] *Jim Bronskill*, Canada a key snooper in huge spy network, Ottawa Citizen, 24.10.2000, http://www.ottawacitizen.com/national/990522/2630510.html.

[114] *James Woolsey*, Remarks at the Foreign Press Center, Transcript, 7.3.2000, http://cryptome.org/echelon-cia.htm.

5.8.2. Déclarations anglaises

Il ressort de différentes questions posées au sein de la chambre des Communes[115], que la station de la RAF de Menwith Hill dépend du ministère anglais de la défense, ce qui n'empêche qu'elle est mise à la disposition du ministère américain de la défense, et en particulier de la NSA[116], un membre du personnel de celle-ci étant le chef de la station[117], en tant qu'installation de communication[118]. Au milieu de l'année 2000, Menwith Hill occupait 415 militaires américains, 5 militaires britanniques, 989 civils américains et 392 civils britanniques, compte non tenu des collaborateurs du GCHQ[119]. La présence des troupes américaines est régie par le traité de l'Atlantique nord et par des accords administratifs spéciaux et secrets[120], qui sont jugés conformes aux relations existant entre les gouvernements du Royaume-Uni et des États-Unis dans le contexte d'une défense commune[121]. La station fait partie intégrante du réseau mondial du ministère américain de la défense, qui défend les intérêts du Royaume-Uni, des États-Unis et de l'OTAN[122].

Le rapport annuel 1999/2000 souligne expressément l'importance que revêt l'étroite collaboration dans le cadre de l'accord UKUSA et la qualité des renseignements qu'elle permet d'obtenir. Il est en particulier dit que si les installations de la NSA devenaient inopérationnelles, le GCHQ pourrait, trois jours plus tard, servir non seulement ses clients britanniques mais aussi ses clients américains[123].

5.8.3. Déclarations australiennes[124]

Martin Brady, directeur de la DSD, service de renseignement australien[125], a confirmé dans une lettre adressée au programme "Sunday" de la chaîne australienne "Channel 9", que la DSD collaborait avec d'autres services de renseignement dans le cadre de l'UKUSA. Dans la même lettre, il a souligné que l'ensemble des installations de renseignement australiennes était géré par les services australiens seuls ou en commun avec les services américains. Dans les cas où ces installations sont utilisées en commun, le gouvernement australien a pleinement connaissance de toutes les activités, et le personnel australien est associé à tous les stades[126].

---

[115] Commons Written Answers, House of Commons Hansard Debates.
[116] 12.7.1995.
[117] 25.10.1994.
[118] 3.12.1997.
[119] 12.5.2000.
[120] 12.7.1995.
[121] 8.3.1999 et 6.7.1999.
[122] 3.12.1997.
[123] Intelligence and Security Committee, Annual Report 1999-2000, Z. 14, présenté au Parlement par le Premier ministre en novembre 2000.
[124] *Martin Brady*, directeur de la DSD, lettre du 16 mars 1999 à Ross Coulthart, Sunday Program, channel 9, http://sunday.ninemsn.com/01_cover_stories/transcript_335.asp; http://sunday.ninemsn.com/01_cover_stories/article_335.asp .
[125] Defence Signals Directorate, Service de renseignement australien gérant le MRE (SIGINT).
[126] *Martin Brady*, directeur de la DSD, lettre du 16 mars 1999 à Ross Coulthart, Sunday Program, channel 9, http://sunday.ninemsn.com/01_cover_stories/transcript_335.asp; http://sunday.ninemsn.com/01_cover_stories/article_335.asp.

5.8.4. Déclarations néo-zélandaises

Comme il a déjà été expliqué au point 5.4.2.2., une publication, de 2000, des services du Premier ministre néo-zélandais concernant les services de la sûreté et du renseignement fait clairement état du partenariat existant entre les services de renseignement de 5 pays – États-Unis, Royaume-Uni, Canada, Australie et Nouvelle-Zélande – et des avantages qu'il présente pour la Nouvelle-Zélande[127].

5.8.5. Déclarations néerlandaises

Le 19 janvier 2001, le ministre néerlandais de la défense a présenté au Parlement néerlandais un rapport sur les aspects techniques et juridiques de l'interception mondiale des systèmes de télécommunications modernes[128]. Le gouvernement néerlandais y défend l'idée que même s'il ne dispose pas lui-même d'éléments de preuve, il juge, compte tenu des informations disponibles auprès de tiers, très plausible l'existence du réseau ECHELON, mais qu'il est possible qu'existent également d'autres systèmes présentant les mêmes possibilités. Il arrive à la conclusion que l'interception à grande échelle des systèmes de télécommunications modernes n'est pas l'apanage des pays parties au système ECHELON et qu'elle est également pratiquée par les responsables d'autres pays.

5.8.6. Déclarations italiennes

Luigi Ramponi, ex-directeur du service de renseignement italien SISMI, ne laisse lui non plus, dans une interview accordée au journal "Il Mondo", subsister aucun doute quant à l'existence d'ECHELON[129]. Ramponi déclare expressément qu'en sa qualité de chef du SISMI, il était au courant de l'existence d'ECHELON. Depuis 1992, il connaissait l'existence d'une forte activité d'écoute des ondes de basse, moyenne et haute fréquences. Lorsqu'il est arrivé au SISMI en 1991, l'essentiel de travail était en rapport avec le Royaume-Uni et les États-Unis.

5.9. Questions au Conseil et à la Commission

Dès le 17 février 1998, le Conseil se vit poser par la député Elly Plooij-van Gorsel[130], une première question générale sur le rapport STOA et sur l'existence d'un système d'interception

---

[127] Domestic and External Secretariat du Department of the Prime Minister and Cabinet de Nouvelle-Zélande Securing our Nation's Safety. How New Zealand manages its security and intelligence agencies (2000). Pour le texte original, cf. supra note du point 5.4.2.2..

[128] Lettre à l'attention de la chambre des députés concernant l'interception à grande échelle des systèmes de télécommunications modernes en date du 19.1.2001.

[129] Francesco Sorti, Dossier. esclusivo. Caso Echelon. Parla Luigi Ramponi. Anche I politici sapevano, Il Mondo, 17.4.1998.

[130] Question écrite P-0501/98 posée par Elly Plooij-van Gorsel (ELDR) au Conseil (17.1.1998). Le 14.5.1997, Jonas Sjöstedt avait déjà posé une question (H-0330/97) sur la résolution du Conseil du 17.1.1995 sur la surveillance légale des télécommunications, où il demandait s'il y avait un lien avec ECHELON. Cette dernière partie de la question n'a pas reçu de réponse. Aux questions de Mihail Papayannakis (G-004/98) et Nel van Dijk (H-0035/98) sur l'activité d'espionnage britannique, il fut répondu le 18.2.1998 que les questions ressortissant aux services de renseignement étaient de la seule compétence des autorités nationales et que le Conseil ne disposait d'aucune information en la matière.

mondial des États-Unis auquel le Royaume-Uni participerait, ainsi que sur les préjudices qui en résulteraient pour les intérêts commerciaux d'entreprises européennes. De nombreuses autres questions sur le même thème suivirent[131]. La présidence y répondit que le Conseil ne disposait lui-même d'aucune information à ce sujet, qu'il n'était pas impliqué dans de telles choses, et qu'il ne pouvait, partant, fournir aucune réponse.

Aux questions similaires posées à la Commission européenne[132], il fut répondu que la Commission avait connaissance du rapport, mais qu'il n'existait ni preuve ni plainte selon laquelle un État membre violerait le traité CE à cet égard[133]. La Commission faisait toutefois preuve de vigilance et défendrait tous les intérêts communautaires non sans continuer à déployer des efforts pour améliorer la sécurité de son réseau informatique[134]. Au cours de la séance plénière du 18 septembre, M. Bangemann, membre de la Commission, déclarait que la Commission ne disposait d'aucune information émanant des États membres ni de citoyens ou d'entreprises selon lesquelles le système d'interception existerait tel qu'il est décrit, ajoutant que si ce système existait bien, il s'agirait naturellement là d'une violation flagrante du droit, des droits individuels des citoyens et bien entendu également une atteinte à la sécurité des États membres, la chose est parfaitement claire, et que dès le moment où on constaterait officiellement un tel état de fait, le Conseil et, cela va de soi, la Commission et le Parlement se devaient de réagir. La Commission agirait également de tout son poids afin d'inciter les États membres à ne pas entrer en possession d'informations par cette voie illégale[135].

---

[131] Question écrite E-0499/98 posée Elly Plooij-van Gorsel (ELDR) au Conseil (27.2.1998), question écrite E-1775/98 posée par Lucio Manisco (GUE-NGL) au Conseil (8.6.1998), question orale H-1086/98, posée au Conseil par Patricia McKenna (16.12.1998), question orale H-1172/98, posée au Conseil par Patricia McKenna (13.1.1999), question orale H-1172/98 posée au Conseil par Inger Schörling (13.1.1999), question orale H-0526/99, posée au Conseil par Pernille Frahm (6.10.1999), question orale H-0621/99, posée au Conseil par Lone Dybkjaer (19.11.1999), etc.

[132] Question écrite E-1039/98 posée par Nel van Dijk (V) à la Commisison (15.5.1998), question écrite E-1306/98 posée par Cristiana Muscardini (NI) à la Commission (15.6.1998), question écrite E-1429/98 posée par Daniela Raschofer (NI) à la Commission (25.6.1998), questions écrites E-1987/98 et E-2329/98 posées par Nikitas Kaklamanis à la Commission (3.9.1998 et 25.9 1998), question écrite 1776/98 posée par Lucio Manisco (GUE/NGL) à la Commission, question écrite 3014/98 posée par Paul Lannoye (V) à la Commission (6.11.1998), question orale H-0547/99 posée par Pernille Frahm à la Commission, question orale H-1067 posée par Patricia McKenna (V) à la Commission (16.12.1998), question orale H-1237/98 posée par Inger Schörling à la Commission (13.1.1999), question orale H-0092/99 posée par Ioannis Theonas à la Commission (13.1.1999), question orale H-0547/99 posée par Pernille Frahm à la Commission (6.10.1999), question orale H-0622/99 posée par Lone Dybkjaer à la Commission (17.12.1999), etc.

[133] Déclaration faite le 25.9.1998 au nom de la Commission, par M. Bangemann, membre de la Commission, en réponse à la question écrite E-1776/98 du député Lucio Manisco (GUE-NGL).

[134] Déclaration faite le 3.9.1998, au nom de la Commission, par M. Santer, Président de la Commission, en réponse à la question écrite E-1987/9.

[135] Débats du Parlement européen, séance du lundi 14.9.1998, point 7 de l'ordre du jour, relations transatlantiques/système ECHELON.

5.10. Rapports parlementaires

5.10.1. Rapports du comité permanent R de contrôle belge

Le comité permanent R de contrôle belge a déjà rendu deux rapports sur le dossier Échelon.

Le troisième chapitre du "Rapport d'activités 1999" est entièrement consacré aux réactions des services belges de renseignement à l'existence éventuelle d'un système Échelon de surveillance des communications. Les auteurs de l'analyse, qui occupe une bonne quinzaine de pages, parviennent à la conclusion que les deux services belges de renseignement, à savoir la Sûreté de l'État et le Service Général du Renseignement (SGR), n'ont obtenu des informations sur ce système qu'au moyen de documents publics.

Le "Rapport complémentaire d'activités 1999" traite du système Échelon d'une manière beaucoup plus approfondie en se prononçant sur les études du STOA. Une partie de ses développements consiste dans l'exposé des conditions techniques et juridiques de l'interception des télécommunications. Il ressort de ses conclusions que le système Échelon existe réellement et permet de capter toutes les informations transmises par satellite (1% environ du nombre total des communications téléphoniques internationales), dès lors qu'est mise en œuvre une recherche par mots clés, et que ses capacités de décryptage sont infiniment supérieures à ce que les Américains veulent bien admettre. Il est permis de mettre en doute les déclarations selon lesquelles aucune activité d'espionnage industriel n'est conduite dans les installations de Menwith Hill. Les auteurs du rapport soulignent expressément l'impossibilité d'établir avec certitude ce que le système Échelon fait ou ne fait pas.

5.10.2. Rapport de la commission de la défense nationale de l'Assemblée nationale française

En France, la commission de la défense nationale a soumis à l'Assemblée nationale un rapport sur les systèmes d'écoute[136]. Lors de sa réunion du 28 novembre 2000, le rapporteur, Arthur Paecht, a présenté à la commission ECHELON du Parlement européen les conclusions de son rapport.

Après avoir traité en détail les différents aspects de la question, le rapporteur, Arthur Paecht, parvient à la conclusion qu'il existe bien un système d'interception nommé ECHELON et qu'il s'agit du seul système multinational connu. Les capacités d'un tel système sont réelles, mais ont atteint leurs limites, non seulement parce que les moyens engagés ne sont plus en rapport avec l'explosion des communications, mais aussi parce que certaines cibles ont appris à se protéger des interceptions.

[136] Rapport d'information, déposé en application de l'article 145 du règlement par la Commission de la défense nationale et des forces armées, sur les systèmes de surveillance et d'interception électroniques pouvant mettre en cause la sécurité nationale, n° 2623 - Assemblée nationale, enregistré à la Présidence de l'Assemblée nationale le 11 octobre 2000.

Le système ECHELON a "divergé" par rapport à ses objectifs initiaux, qui étaient liés au contexte de la guerre froide. Aussi n'est-il pas impossible que des informations recueillies soient utilisées à des fins politiques et économiques contre certains membres de l'OTAN.

ECHELON peut constituer un danger pour les libertés fondamentales. À ce titre, son existence pose de nombreux problèmes qui appellent des réponses appropriées. Il serait vain d'imaginer que les pays membres du réseau vont cesser leurs activités. Plusieurs indices incitent à croire qu'un nouveau système s'est constitué pour dépasser les limites d'ECHELON grâce à de nouveaux moyens et sans doute de nouveaux partenariats.

5.10.3. Rapport de la commission parlementaire italienne des services d'information et de sécurité ainsi que de la sûreté de l'État

En Italie, la commission parlementaire des services d'information et de sécurité a présenté au président du Parlement, le 19 décembre 2000, un rapport sur le rôle des services d'information et de sécurité dans le cas ECHELON[137].

Les conclusions relatives à l'existence d'un système appelé ECHELON sont vagues. Selon le rapport, il a été en grande partie exclu lors des auditions au sein de la commission que pouvait exister un système d'interception intégré de ce nom, qui aurait été mis en place par les cinq pays parties à l'accord UKUSA (États-Unis, Royaume-Uni, Australie, Nouvelle-Zélande et Canada) et qui servirait à intercepter les communications dans le monde entier. S'il était établi qu'il y avait une coopération plus étroite entre les pays anglo-saxons, les enquêtes de la commission ne permettaient cependant pas d'affirmer que cette coopération portait sur la création d'un système d'interception intégré ou d'un système d'interception à l'échelle mondiale. Selon la Commission, il était probable que l'appellation ECHELON désignait un stade du développement technologique dans le domaine de la technique d'interception satellitaire. Il est expressément constaté que le service secret italien SISMI a exclu l'existence, à l'époque, d'un procédé de reconnaissance automatique de mots prononcés au cours de conversations et constaté, dès lors, qu'une interception ciblée de conversations contenant ces mots-clés n'était pas possible.

[137] "Il ruolo dei servizi di informazione e sicurezza nel caso 'Echelon'." Relazione del comitato parlamentare per i servizi di informatione e sicurezza e per il segreto di stato. Approvata nella seduta del 29 novembre 2000. Trasmessa alle Presidenze il 19 dicembre 2000.

6. Peut-il exister d'autres systèmes d'interception mondiaux?

6.1. Conditions nécessaires pour un tel système

6.1.1. Conditions technico-géographiques

Pour pouvoir intercepter, à l'échelle mondiale, des communications internationales acheminées par les satellites de la première génération, des stations de réception sont indispensables dans la zone atlantique, dans la zone de l'océan Indien et dans la zone de l'océan Pacifique. Pour la génération plus récente de satellites, permettant une émission par sous-région, il faut encore respecter d'autres conditions quant à la position géographique des stations d'interception si l'objectif consiste à capter l'ensemble des communications transmises par satellite.

Un autre système d'interception fonctionnant à l'échelle mondiale doit installer ses stations ailleurs que dans les territoires relevant des pays UKUSA.

6.1.2. Conditions politico-économiques

La mise en place d'un tel système d'interception fonctionnant à l'échelle mondiale doit cependant également présenter un intérêt économique et politique pour le ou les exploitants. Le ou les bénéficiaires d'un tel système doivent avoir des intérêts économiques et militaires ou d'autres intérêts en termes de sécurité, ou à tout le moins croire qu'ils font partie des puissances mondiales. Dès lors, le cercle des pays concernés se limite, pour l'essentiel, à la Chine et aux pays du G8, sans les États-Unis et le Royaume-Uni.

6.2. France

Dans les trois zones précitées, la France possède des territoires, départements et collectivités locales qui lui sont propres.

Dans l'Atlantique, il y a, à l'est du Canada, Saint-Pierre-et-Miquelon (65° O / 47° N), au nord-est de l'Amérique du Sud, la Guadeloupe (61° O / 16° N) et la Martinique (60° O / 14° N) ainsi qu'au large de la côte nord-est de l'Amérique du Sud, la Guyane française (52° O / 5° N).

Dans la zone de l'océan Indien, il y a, à l'est de l'Afrique australe, Mayotte (45° E / 12° S) et La Réunion (55° E / 20° S), ainsi que tout au sud, les terres Australes et Antarctiques françaises. Dans la zone du Pacifique, on trouve la Nouvelle-Calédonie (165° E / 20° S), Wallis et Futuna (176° O / 12° S), ainsi que la Polynésie française (150° O / 16° S).

S'agissant de l'existence éventuelle de stations du service de renseignement français – la DGSE (Direction générale de la sécurité extérieure) – dans ces régions d'outre-mer, les renseignements sont peu nombreux. Selon certains journalistes français[138], il existe des stations à Kourou (Guyane française), ainsi qu'à Mayotte. Aucune donnée précise n'est disponible en ce qui concerne la grandeur de ces stations ainsi que le nombre ou les dimensions des antennes satellitaires. En France, d'autres stations existeraient à Domme (près de Bordeaux) et aux Alluetts-le-Roi (près de Paris). Jauvert estime à 30 au total le nombre des antennes satellitaires. L'écrivain Erich Schmidt-Eenboom[139] affirme qu'une station serait également en service en Nouvelle-Calédonie et que le service de renseignement allemand utiliserait dans une certaine mesure cette installation.

En théorie, la France, qui réunit non seulement les conditions géographiques mais aussi les conditions techniques et financières, pourrait également exploiter un système d'interception fonctionnant à l'échelle mondiale. Votre rapporteur ne dispose toutefois pas de suffisamment d'informations de sources publiques pour pouvoir l'affirmer sérieusement.

6.3. Russie

La FAPSI (Direction des transmissions présidentielles – Federalnoye Agentstvo Pravitelstvennoy Svyazi), le service de renseignement russe responsable pour la sécurité des communications et le SIGINT, exploite, conjointement avec le GROU (Service de renseignement de l'armée), des stations au sol en Lettonie, au Vietnam et à Cuba.

Conformément à la base juridique, l'objectif de la FAPSI consiste à recueillir des informations d'ordre politique, économique, militaire et technico-scientifique aux fins de promouvoir le développement économique ainsi que le progrès scientifico-technique et militaire[140]. De plus, le directeur de la FAPSI a constaté en 1997 que sa fonction première était l'interception des communications étrangères codées ainsi que l'écoute mondiale[141].

---

[138] *Jean Guisnel*, L'espionnage n'est plus un secret, The Tocqueville Connection, 10.7.1998.
Vincent Jauvert, Espionnage, comment la France écoute le monde, Le nouvel Observateur, 5.4.2001, N° 1900, pp. 14 et ss.

[139] *Erich Schmidt-Eenboom,* Streng Geheim, Museumsstiftung Post und Telekommunikation Heidelberg, 1999.

[140] Loi de la Fédération de Russie sur le renseignement étranger adoptée par la Douma le 8.12.1995, sections 5 et 11.

[141] Citation in *Gordon Bennett*, Conflict Studies and Research Center, The Federal Agency of Government Communications and Information, août 2000, http://www.csrc.ac.uk/pdfs/c105.pdf

Dans la zone de l'Atlantique, il y a la station cubaine de Lourdes (82° O / 23° N), qui est exploitée en commun avec le service de renseignement cubain. Par l'intermédiaire de cette station, la Russie recueille à la fois des informations stratégiques, militaires et commerciales[142]. Pour la zone de l'océan Indien, il y a des stations en Russie, à propos desquelles on ne dispose d'aucune information précise. Une autre station située à Skrunda (Lettonie) a été fermée en 1998[143]. Dans la zone du Pacifique, il y aurait une station dans la baie de Cam Ranh (République socialiste du Vietnam). On ne sait rien de précis sur ces stations ni sur le nombre et les dimensions des antennes.

Ces stations et celles qui existent en Russie même permettent en théorie une couverture mondiale. En l'occurrence, les informations disponibles sont néanmoins également insuffisantes pour pouvoir affirmer avec certitude quelque chose.

6.4. Autres pays du G8 et Chine

Les autres pays du G8 et la Chine n'ont aucun territoire propre ni véritable allié dans les régions du monde nécessaires pour exploiter un système d'interception mondial.

[142] Citation in *Gordon Bennett*, UK Ministry of Defence, The Federal Agency of Government Communications and Information, et page d'accueil de la Federation of American Scientists

[143] Page d'accueil de la Federation of American Scientists (FAS), http://www.fas.org

7. Compatibilité d'un système d'interception des communications du type "ECHELON" avec le droit de l'Union européenne

7.1. Commentaires sur la question

Selon son mandat, la commission est notamment expressément chargée de vérifier la compatibilité d'un système d'interception des communications du type ECHELON avec le droit communautaire[144]. Elle doit en particulier s'assurer qu'un tel système est compatible avec les deux directives relatives à la protection des données (95/46/CE et 97/66/CE, ainsi qu'avec l'article 286 du traité CE et l'article 8, paragraphe 2, du traité sur l'Union européenne.

Il semble nécessaire d'envisager cette question sous deux angles différents. Une première approche procède de la preuve par indices du chapitre 5, dont il ressort que le système baptisé ECHELON a été conçu comme un système d'interception des communications, qui par la collecte et l'exploitation des données communiquées, doit fournir aux services secrets américain, canadien, australien, néo-zélandais et britannique des informations sur des faits à l'étranger. En l'occurrence, il s'agit donc d'un instrument d'espionnage classique des services de renseignement extérieur[145]. Aussi faut-il, dans un premier temps, examiner la question de la compatibilité d'un tel système de renseignement avec le droit de l'Union.

Par ailleurs, dans le rapport qu'il a présenté au STOA, Campbell formule une accusation, à savoir que ce système serait utilisé aux fins de l'espionnage de concurrence, ce qui serait à l'origine de préjudices graves pour l'économie des pays européens. De plus, selon certaines déclarations faites par l'ancien directeur de la CIA, R. James Woosley, les États-Unis espionneraient des entreprises européennes, et ce uniquement toutefois pour rétablir un marché équitable, dès lors qu'autrement les contrats ne sont obtenus que grâce à la corruption[146]. S'il était exact que les systèmes sont utilisés aux fins de l'espionnage de concurrence, alors la question de la compatibilité avec le droit communautaire se poserait de nouveau. Ce deuxième aspect doit donc être étudié séparément.

7.2. Compatibilité d'un système de renseignement avec le droit de l'Union européenne

7.2.1. Compatibilité avec le droit communautaire

En principe, les activités et mesures concernant la sûreté de l'État ou les poursuites pénales ne relèvent pas du champ d'application du traité CE. Dans la mesure où conformément au principe de la compétence restreinte, la Communauté européenne ne peut agir que là où elle est

[144] Cf. à ce propos chapitre 1, point 1.3. supra.
[145] Cf. à ce propos chapitre 2 supra..
[146] Cf. à ce propos chapitre 5, points 5.6 et 5.8.

formellement habilitée à le faire, elle a exclu ces différents domaines du champ d'application des directives relatives à la protection des données, fondées sur le traité CE et, en particulier, son article 95 (ex-article 100A). La directive 95/46/CE du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données[147] et la directive 97/66/CE du Parlement européen et du Conseil concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications[148] ne s'appliquent pas "en tout état de cause aux traitements[149]/activités [150] concernant la sécurité publique, la défense, la sûreté de l'État (y compris la prospérité économique de l'État lorsque ces traitements sont des questions de sûreté de l'État/lorsqu'il s'agit d'activités liées à la sûreté de l'État) et les activités de l'État relatives à des domaines du droit pénal/ou aux activités de l'État dans les domaines relevant du droit pénal". La proposition de directive du Parlement européen et du Conseil concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques[151], dont le Parlement est actuellement saisi, fait également sien ce libellé. Aussi, la participation d'un État membre à un système d'interception aux fins de la sûreté de l'État n'est-elle pas incompatible avec les directives communautaires relatives à la protection des données.

Il ne saurait pas davantage être question d'une violation de l'article 286 du traité CE, qui étend le champ d'application des directives relatives à la protection des données au traitement des données par les organes et institutions communautaires. Il en va de même pour le règlement (CE) n° 45/2001 du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données[152]. Ce règlement ne s'applique également que là où ces organes et institutions agissent dans le cadre du traité CE[153]. Pour éviter tout malentendu, il convient de souligner expressément ici qu'une participation des organes et institutions communautaires à un système d'interception n'a jamais été évoquée, et que votre rapporteur ne dispose d'aucun élément lui permettant de croire à une telle participation.

7.2.2. Compatibilité avec d'autres dispositions législatives de l'Union européenne

Pour les domaines ressortissant aux titres V (politique étrangère et de sécurité commune) et VI (coopération policière et judiciaire en matière pénale), il n'existe aucune disposition concernant la protection des données qui soit comparable avec les directives communautaires. Le Parlement européen a souligné à plusieurs reprises déjà qu'il était impérieux d'agir dans ce domaine[154].

---

[147] JO L 281 du 23.11.1995, p. 31.
[148] JO L 24 du 30.1.1998, p. 1.
[149] Directive 95/46/CE, art. 3, par. 2.
[150] Directive 97/66/CE, art. premier, par. 3.
[151] COM(2000) 385, JO C 365 E, p. 223.
[152] Règlement (CE) n° 45/2001, JO L 8 du 12.1.2001, p. 1.
[153] Art. 3, par. 1; cf. également le considérant 15: "lorsque ce traitement est effectué par les institutions et organes communautaires pour l'exercice d'activités situées hors du champ d'appplication du présent règlement, en particulier celles prévues aux titres 5 et 6 du traité sur l'Union européenne, la protection des libertés et droits fondamentaux des personnes est assurée dans le respect de l'article 6 du traité sur l'Union européenne. (…)".
[154] Cf. par exemple le paragraphe 25 de la résolution sur le projet de plan d'action du Conseil et de la Commission concernant les modalités optimales de mise en œuvre des dispositions du traité d'Amsterdam relatives à l'établissement d'un espace de liberté, de sécurité et de justice (13844/98 – C4-0692/98 – 98/0923(CNS)), JO C

Dans ces domaines, la protection des droits et libertés fondamentaux des personnes est garantie par les articles 6 et 7, et en particulier par l'article 6, paragraphe 2, du traité sur l'Union européenne, par lequel l'Union s'engage à respecter "les droits fondamentaux, tels qu'ils sont garantis par la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales (…) et tels qu'ils résultent des traditions constitutionnelles communes aux États membres". Ainsi, si les États membres sont tenus de respecter les droits fondamentaux et en particulier la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales (cf. à ce propos infra chapitre 8), l'Union est elle aussi tenue de respecter les droits fondamentaux dans l'exercice de ses compétences législatives et administratives. Dès lors qu'il n'existe toutefois pas jusqu'ici, dans l'Union européenne, une réglementation concernant la légalité de la surveillance des télécommunications aux fins de la protection de la sûreté de l'État et du renseignement[155], la question de la violation de l'article 6, paragraphe 2, du traité sur l'Union européenne ne se pose pas directement.

7.3. Problème de la compatibilité en cas d'utilisation du système aux fins de l'espionnage de concurrence

Si un État membre prêtait assistance à un système d'interception, destiné entre autres à également espionner les entreprises, en permettant d'utiliser à cet effet ses propres services de renseignement ou en mettant son territoire à la disposition de services de renseignement étrangers, alors, il pourrait très bien y avoir violation du droit communautaire. En effet, aux termes de l'article 10 du traité CE, les États membres ont un devoir de loyauté générale et doivent en particulier s'abstenir "de toutes mesures susceptibles de mettre en péril la réalisation des buts du (…) traité." Même dans le cas où l'interception de télécommunications ne se ferait pas au profit de l'économie nationale (ce qui au demeurant aurait un effet comparable à celui d'une aide d'État et serait dès lors incompatible avec l'article 87 du traité CE), mais bien au profit de pays tiers, une telle activité serait fondamentalement contraire au principe du marché commun à la base du traité CE, dans la mesure où elle équivaudrait à une distorsion de concurrence.

De l'avis de votre rapporteur, une telle attitude représenterait en outre une violation de la directive concernant le traitement des données à caractère personnel et la protection de la vie

---

219 du 30.7.1999, pp. 61 et ss.

[155] En matière de surveillance des télécommunications, il n'existe actuellement dans l'Union européenne que deux actes, aucun d'eux n'ayant trait à la question de la légalité:
– la résolution du Conseil, du 17 janvier 1995, relative à l'interception légale des télécommunications (JO C 329 du 4.11.1996), dont l'annexe constitue un condensé des besoins des autorités compétentes pour la réalisation technique des mesures d'interception légale dans les systèmes modernes de télécommunications, et
– l'acte du Conseil du 29 mai 2000 établissant, conformément à l'article 34 du traité sur l'Union européenne, la convention relative à l'entraide judiciaire en matière pénale entre les États membres de l'Union européenne (JO C 197 du 12.7.2000, p. 1, art. 17 et ss.), qui arrête les conditions dans lesquelles l'entraide judiciaire en matière pénale doit être possible pour ce qui est de l'interception des télécommunications. Il n'en résulte aucune atteinte pour les droits de ceux dont les communications sont interceptées, l'État où ceux-ci se trouvent ayant alors toujours la possibilité de refuser l'entraide judiciaire, lorsque le droit national s'y oppose.

privée dans le secteur des télécommunications[156] dès lors que la question de l'applicabilité des directives doit être résolue sur la base de considérations fonctionnelles et non organisationnelles. Et ce non seulement en raison du libellé des dispositions relatives au champ d'application mais aussi de l'esprit de la loi. Si des services de renseignement utilisent leurs capacités aux fins de l'espionnage de concurrence, leur activité n'est pas en rapport avec la sûreté de l'État ou des poursuites pénales, mais elle vise d'autres objectifs et entre dès lors pleinement dans le champ d'application de la directive. Aux termes de l'article 5 de celle-ci, les États membres sont tenus de garantir la confidentialité des communications, et en particulier d'interdire "à toute autre personne que les utilisateurs (…) d'écouter, d'intercepter, de stocker les communications ou de les soumettre à quelque autre moyen d'interception ou de surveillance (…)". Aux termes de l'article 14, des exceptions ne sont possibles que dans le cas où elles sont nécessaires "pour sauvegarder la sûreté de l'État, la défense (…) et la poursuite d'infractions pénales (…)". L'espionnage économique n'étant pas un motif légitime d'exception, il y aurait alors violation du droit communautaire.

7.4. Conclusions

En résumé, il est possible de dire qu'en principe, dans la situation juridique actuelle, un système de renseignement du type ECHELON ne saurait être contraire au droit de l'Union, dès lors qu'il ne présente aucun rapport avec des éléments du droit de l'Union justifiant son incompatibilité. Il en va toutefois uniquement ainsi tant que le système est utilisé exclusivement aux fins de garantir la sûreté de l'État au sens large. S'il est par contre détourné de ses objectifs pour espionner des entreprises étrangères, il y a bien infraction au droit communautaire. Et si un État membre participait à une activité de ce type, il violerait le droit communautaire.

[156] Directive 97/66/CE, JO L 24 du 30.1.1998, p. 1.

8. La surveillance des communications par les services de renseignements est-elle compatible avec le droit fondamental au respect de la vie privée

8.1. La surveillance des communications, atteinte au droit fondamental au respect de la vie privée

Toute écoute de communication, à commencer par l'interception de données par des services de renseignements à cette fin[157], représente une atteinte profonde à la vie privée de la personne. L'écoute illimitée par la puissance publique n'est admissible que dans un "État policier". Dans les États membres de l'UE, qui sont des démocraties évoluées, la nécessité pour les organes de l'État, c'est–à–dire aussi pour les services de renseignements, de respecter la vie privée est incontestée et généralement inscrite dans les différentes constitutions nationales. La vie privée bénéficie donc d'une protection particulière et des possibilités d'intervention ne sont accordées qu'après évaluation des biens protégés par des dispositions légales et dans le respect du principe de proportionnalité.

Dans les pays UKUSA aussi, on est conscient du problème. Les dispositions de protection prévues visent toutefois le respect de la vie privée des ressortissants nationaux, de sorte que le citoyen européen est généralement exclu du bénéfice de celles–ci. Aux États–Unis, dans les dispositions qui définissent les conditions de la surveillance électronique, aux intérêts de l'État en ce qui concerne le bon fonctionnement des services de renseignements ne fait pas pendant le souci d'une protection générale efficace des droits fondamentaux, mais la nécessaire protection de la vie privée des "citoyens américains".[158]

8.2. La protection de la vie privée garantie par les conventions internationales

Le respect de la vie privée en tant que droit fondamental est inscrit dans de nombreuses conventions de droit international public[159]. Au plan mondial, le pacte international relatif aux

---

157 Tribunal constitutionnel fédéral, 1 BvR 2226/94 du 14.7.1999, n° 187 "Eingriff ist [...] schon die Erfassung selbst, insofern sie die Kommunikation für den Bundesnachrichtendienst verfügbar macht und die Basis des nachfolgenden Abgleichs mit den Suchbegriffen bildet."

158 Cf. rapport au Congrès des États–Unis de fin février 2000 "Legal Standards for the Intelligence Community in conducting Electronic Surveillance", http://www.fas.org/irp/nsa/standards.html, qui fait référence au Foreign Intelligence Surveillance Act (FISA), reproduit au titre 50 chapitre 36 U.S.C. § 1801 et ss. et à l'Exec. Order No. 12333, 3 C.F.R. 200 (1982), reproduit au titre 50, chapitre 15 U.S.C. § 401 et ss., http://www4.law.cornell.edu/uscode/50/index.html.

159 Art. 12 Déclaration universelle des droits de l'homme; Art 17, Pacte des Nations unies relatif aux droits civils et politiques; Art. 7, Charte de l'UE, Art. 8, convention européenne des droits de l'homme, recommandation du Conseil de l'OCDE sur des lignes directrices pour la sécurité des systèmes informatiques adoptée les 26 et 27.11.1993 C(92) 188/Final; Art 7 Convention du Conseil de l'Europe sur la protection des personnes dans le domaine du traitement automatique des données à caractère personnel; cf. à ce propos l'étude commandée par le STOA "Development of surveillance tehnology and risk of abuse of economic information", Vol 4/5: The legality of the interception of electronic communications: A concise survey of the principal legal issues and instruments under international, European and national law (Chris Elliot), octobre 1999, 2.

droits civils et politiques[160], conclu en 1966 dans le cadre de l'ONU, garantit en son article 17 la protection de la vie privée. Tous les pays UKUSA ont souscrit aux décisions de la commission des droits de l'homme instituée conformément à l'article 41 et qui examine les violations de la convention, et ce dès lors qu'il y a plainte d'autres pays. Le protocole additionnel[161], qui étend la compétence de la commission aux recours individuels, n'a cependant pas été signé par les États–Unis, de sorte qu'il est impossible à une personne privée de s'adresser à la commission des droits de l'homme en cas de violation de la convention par les États-Unis.

Au niveau de l'UE, on s'est efforcé de mettre en place une protection européenne particulière des droits fondamentaux en élaborant une charte des droits fondamentaux de l'UE. L'article 7 de celle-ci, qui concerne le respect de la vie privée et familiale, régit même expressément le droit au respect des communications[162]. De plus, l'article 8 régit le droit fondamental à la protection des données à caractère personnel. Cette disposition protégerait la personne au cas où des données la concernant seraient traitées (par la voie informatique ou non), ce qui est généralement le cas en cas d'écoute et l'est toujours en cas d'interception par d'autres moyens.

A ce jour, la Charte n'a pas été incorporée au traité. Elle n'est contraignante que pour les trois institutions qui y ont souscrit dans la déclaration solennelle en marge du Conseil européen de Nice: Conseil, Commission et Parlement européen. À la connaissance du rapporteur, celles-ci ne sont pas engagées dans des activités de services secrets. Même si l'incorporation au traité donnait à la Charte tous ses effets, il faut tenir compte de son champ d'application limité. Aux termes de l'article 51, ces dispositions "s'adressent aux institutions et organes de l'Union ... ainsi qu'aux États membres uniquement lorsqu'ils mettent en œuvre le droit de l'Union". La Charte s'appliquerait donc en plus de l'instrument représenté par l'interdiction d'aides publiques contraires à la concurrence (voir chapitre 7, point 7.3).

Le seul instrument efficace au plan international en matière de protection globale de la vie privée est constitué par la convention européenne relative aux droits de l'homme.

8.3. Les dispositions de la convention européenne des droits de l'homme

8.3.1. L'importance de la convention dans l'UE

La protection des droits fondamentaux assurée par la convention revêt une importance particulière dans la mesure où la convention a été ratifiée par tous les États membres de l'UE, de sorte qu'elle assure un niveau de protection uniforme en Europe. Les États partie à cette convention se sont engagés en droit international à garantir les droits reconnus par la convention et à se soumettre à la juridiction de la Cour européenne des droits de l'homme de Strasbourg. Celle-ci peut vérifier la conformité des réglementations nationales par rapport à la convention. En cas de violation des droits de l'homme, elle peut condamner les États signataires et les contraindre à payer des dédommagements. L'importance de la convention se trouve encore accrue du fait que la Cour de justice des Communautés européennes l'a consultée à plusieurs

[160] Pacte international relatif aux droits civils et politiques, adopté par l'AG des Nations unies le 16. 12. 1966.
[161] Protocole facultatif au pacte international relatif aux droits civils et politiques, adopté par l'AG des Nations unies le 16.12.1966.
[162] "Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de ses communications".

reprises dans le contexte de vérifications de dispositions législatives par rapport aux principes généraux du droit des États membres. Le traité d'Amsterdam (article 6, paragraphe 2, du traité UE) prévoit en outre l'obligation pour l'UE de respecter les droits fondamentaux tels qu'ils sont garantis par la convention.

8.3.2. Portée de la protection offerte par la convention

Les droits inscrits dans la convention sont des droits de l'homme universels qui ne sont donc pas liés à la nationalité. Ils doivent être reconnus à toutes les personnes soumises à la juridiction des États signataires. Cela signifie que les droits de l'homme doivent dans tous les cas êtres accordés sur l'ensemble du territoire national, des exceptions locales constituant une violation de la convention. De plus, ces droits s'appliquent aussi hors du territoire national des États signataires dès lors que la puissance publique s'y exerce. Les droits garantis par la convention vis–à–vis d'un État signataire sont donc reconnus aux personnes hors du territoire national dès lors qu'un État signataire porte atteinte à la vie privée hors du territoire national[163].

Ce dernier aspect est particulièrement important dans le contexte qui nous intéresse car le problème des droits fondamentaux dans le domaine de la surveillance des télécommunications présente la particularité que l'État qui est responsable de la surveillance, la personne surveillée et le processus d'interception lui–même ne sont pas présents en un même lieu. Cela s'applique notamment aux communications internationales mais aussi dans certains cas aux communications nationales lorsque le transport de l'information s'effectue via l'étranger. C'est même la règle en ce qui concerne l'action des services de renseignements à l'étranger. Par ailleurs, il ne peut être exclu que les informations obtenues grâce à la surveillance par un service de renseignements soient transmises à d'autres pays.

8.3.3. Surveillance des télécommunications au regard de l'article 8 de la convention

L'article 8, paragraphe 1, de la convention dispose que "toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance". Il n'est pas fait mention expressément de la protection des communications téléphoniques et des télécommunications, mais en vertu de la jurisprudence de la Cour des droits de l'homme, ces aspects sont également couverts par les notions de vie privée et de correspondance et bénéficient à ce titre de la protection de l'article 8 de la convention[164]. La protection des droits fondamentaux s'étend non seulement au contenu des communications, mais aussi à l'enregistrement de données extérieures. Cela signifie que même si un service de renseignements n'enregistre que des données telles que heure et durée des communications ou encore numéros composés, il s'agit là d'une atteinte à la

[163] CEDH Loizidou/Turquie, 23.3.1995, n° 62 avec d'autres éléments à l'appui "...the concept of 'jursidiction' under this provision is not restricted to the national territory of the High Contracting Parties.[...] responsibility can be involved because of acts of their authorities, whether performed within or outside national boundaries, which produce effects outside their own territory" avec référence à la CEDH, Drozd und Janousek, 26.6.1992, n° 91. Pour plus de détails, cf. *Francis G.* Jacobs, *Robin C. A. White,* The European Convention on Human Rights[2], Clarendon Press (1996), 21 et ss, *Jochen Abr. Frowein, Wolfgang Peukert,* Europäische Menschenrechtskonvention, N. P. Engel Verlag (1996), Rz 4 et ss.

[164] CEDH, Klass et autres, 6.9.1978, n° 41.

vie privée[165].

Le droit qui est reconnu à l'article 8, paragraphe 2, de la convention n'est pas illimité. Des atteintes au droit fondamental au respect de la vie privée sont admissibles dès lors qu'elles disposent d'une base juridique dans le droit national[166]. Le droit doit être accessible à tous et prévisible dans ses effets[167].

Les États membres ne disposent donc pas d'une liberté totale pour organiser ces ingérences. L'article 8 de la convention n'autorise celles-ci que pour réaliser les objectifs énumérés au paragraphe 2, à savoir notamment sécurité nationale, sûreté publique, prévention d'infractions pénales ainsi que bien–être économique du pays[168], ce qui ne justifie toutefois pas l'espionnage économique car seules les interventions nécessaires dans une société démocratique sont couvertes. Pour toute intervention, il faut recourir au moyen minimal permettant d'atteindre l'objectif et, en outre, prévoir des garanties suffisantes contre les abus.

8.3.4. Importance de l'article 8 de la convention sous l'angle des activités des services de renseignements

Du point de vue de l'organisation conforme aux droits fondamentaux des activités des services de renseignements, ces principes généraux signifient que s'il apparaît nécessaire, pour assurer la sécurité nationale, d'autoriser les services de renseignements à intercepter le contenu de télécommunications ou au moins des données relatives aux communications, cela doit être prévu par le droit national et les dispositions afférentes doivent être accessibles à tous. Les conséquences de ces dispositions doivent être prévisibles pour chacun, non toutefois sans tenir compte des exigences du secret. C'est ainsi que dans un arrêt relatif à la conformité avec l'article 8 de contrôles secrets visant des fonctionnaires dans des domaines touchant à la sécurité nationale, la Cour des droits de l'homme a constaté que l'aspect de prévisibilité dans ce cas particulier ne peut être identique à ce qu'il est dans d'autres domaines[169]. Elle a demandé dans ce cas aussi que les dispositions juridiques précisent dans quelles circonstances et conditions la puissance publique peut porter une atteinte secrète et, partant, potentiellement dangereuse, à la vie privée[170].

Une organisation conforme aux droits de l'homme des activités des services de renseignements

---

165 CEDH, Malone, 2.8.1984, n° 83 et suivants; Davy, B/Davy/U, Aspekte staatlicher Informationssammlung und Art 8 MRK, JBl 1985, 656.

166 Selon la jurisprudence de la Cour des droits de l'homme (voir notamment Sunday Times, 26.4.1979, p. 46 ss, Silver ua, 25.3.1983, p.85 ss) la notion de "loi" visée à l'art. 8, par. 2 englobe non seulement les lois au sens formel, mais aussi les dispositions de catégories inférieures, c'est–à–dire aussi le droit non écrit. Cela suppose toutefois que le justiciable ait la possibilité de déterminer dans quelles circonstances une ingérence est possible. Pour plus de détails, Wolfgang Wesseley, Das Fernmeldegeheimnis – ein unbekanntes Grundrecht? ÖJZ 1999, 491 ss, 495.

167 Silver et autres, 25.3.1983, Z 87 et ss.

168 L'argument du bien–être économique a été admis par la Cour dans un cas où il s'agissait de la communication de données médicales importantes du point de vue de l'octroi de prestations publiques: M.S./Suède, 27.8.1997, p.38; ainsi que dans un cas concernant l'expulsion des Pays–Bas d'une personne qui était dépendante de la sécurité sociale après que la justification de son permis de séjour fut devenue caduque Ciliz/Pays-Bas, 11.7.2000, p. 65.

169 CEDH, Leander, 26.3.1987, p. 51.

170 CEDH, Malone, 2.8.1984, p. 67.

suppose que l'on tienne compte de l'aspect suivant: si la sécurité nationale constitue une justification, celle–ci est toutefois soumise au principe de proportionnalité, conformément à l'article 8, paragraphe 2 de la convention. Même la sécurité nationale ne peut justifier des ingérences que dans le cas où celles–ci apparaissent nécessaires au sein d'une société démocratique. À cet égard, la Cour des droits de l'homme a indiqué que le souci de l'État de protéger la sécurité nationale doit être mis en balance avec les intérêts de la personne en ce qui concerne le respect de la vie privée[171]. Les ingérences ne sont certes pas limitées à ce qui est indispensable mais il ne suffit pas qu'elles soient opportunes ou souhaitables[172]. L'idée selon laquelle l'interception de toute télécommunication constituerait la meilleure protection contre la criminalité organisée serait contraire à l'article 8 de la convention même si cela était prévu par le droit national.

Il faut en outre prévoir des possibilités de contrôle plus importantes eu égard au caractère particulier des activités des services de renseignements qui supposent le secret et, par voie de conséquence, une certaine mise en balance des intérêts. La Cour a souligné qu'un système de surveillance secret destiné à garantir la sécurité nationale porte en soi le risque de saper ou de détruire la démocratie sous prétexte de la défendre et qu'il faut par conséquent des garanties appropriées et efficaces contre de tels abus[173]. Les activités légitimes des services de renseignements ne sont conformes aux droits fondamentaux que si l'État signataire de la convention a prévu des systèmes de contrôle suffisants et d'autres garanties contre les abus. À cet égard, la Cour a fait observer, dans le contexte des activités des services de renseignements suédois, qu'elle accordait une importance particulière à la présence de députés au sein de l'organe de contrôle policier ainsi qu'à la surveillance exercée par le ministre de la justice, par le médiateur parlementaire et par la commission juridique du Parlement. Dans ces conditions, il apparaît critiquable que la France, la Grèce, l'Irlande, le Luxembourg et l'Espagne ne disposent pas de commissions parlementaires chargées de contrôler les services secrets[174], pas plus que de système de contrôle comparable au médiateur parlementaire des pays nordiques[175]. Le rapporteur se félicite par conséquent des efforts déployés par la commission de la défense de l'Assemblée nationale française pour instituer une commission de contrôle[176], d'autant que la France dispose de capacités de renseignements notables, tant du point de vue technique que du point de vue géographique.

---

171 CEDH, Leander, 26.3.1987, Z 59, Sunday Times, 26.4.1979, p. 46 ss.

172 CEDH, Silver et autres, 24.10.1983, Z 97.

173 CEDH, Leander, 26.3.1987, p. 60.

174 Le rapporteur sait que ni le Luxembourg ni l'Irlande ne disposent ni de services de renseignements à l'étranger ni de SIGINT. La nécessité d'une instance de contrôle particulière ne concerne que les activités de renseignements à l'intérieur du pays.

175 Au sujet du contrôle des services de renseignements dans les États membres, voir chapitre 9.

176 Proposition de loi tendant à la création de délégations parlementaires pour le renseignement, et rapport afférent du député Arthur Paecht, Rapport fait au nom de la Commission de la défense nationale et des forces armées sur la proposition de loi (N° 1497) de M. Paul Quilès et plusieurs de ses collègues tendant à la création d'une délégation parlementaire pour les affaires de renseignement, enregistré à la Présidence de l'Assemblée nationale le 23 novembre 1999.

8.4. Obligation de vigilance vis–à–vis des activités de services de renseignements étrangers

8.4.1. Caractère inadmissible d'une violation de l'article 8 de la convention liée à l'intervention de services de renseignements étrangers

Comme il a été exposé plus haut, les parties signataires doivent satisfaire à plusieurs conditions pour que les activités de leurs services de renseignements soient compatibles avec l'article 8 de la convention. Il est évident que les services de renseignements ne peuvent se soustraire à ces obligations en recourant aux services d'autres organismes de renseignements soumis à des dispositions moins rigoureuses. S'il en était autrement, le principe de légalité et ses deux composantes – possibilité d'accès et prévisibilité – se trouverait privé de ses effets cependant que la jurisprudence de le Cour serait vidée de sa substance.

Cela signifie d'une part que l'échange de données entre services de renseignements n'est admissible que dans une mesure limitée. Un service de renseignements ne peut solliciter d'un autre des données que si lesdites données peuvent être obtenues dans des conditions prévues par le droit national. Le rayon d'action défini par la loi ne peut être étendu à travers des accords avec d'autres services. De la même manière , un service de renseignements ne peut intervenir sur instructions d'un service de renseignements étranger qu'à condition d'avoir établi que lesdites activités sont conformes au droit national. Même si les informations sont destinées à un pays étranger, cela ne change rien au fait qu'une ingérence que le justiciable ne pouvait prévoir est contraire à ses droits fondamentaux.

Par ailleurs, les pays signataires de la convention ne peuvent autoriser des services de renseignements étrangers à intervenir sur leur territoire dès lors que l'on peut soupçonner que leurs activités ne sont pas conformes aux dispositions de la convention[177].

8.4.2. Conséquences sous l'angle des activités de services de renseignements extra–européens sur le territoire de pays signataires de la convention

8.4.2.1. Jurisprudence de la Cour européenne des droits de l'homme

En ratifiant la convention, les signataires se sont engagés à soumettre l'exercice de leur souveraineté à une vérification du respect des droits fondamentaux. Ils ne peuvent se soustraire à cette obligation en renonçant à leur souveraineté. Ils conservent la responsabilité de leur territoire ainsi que leurs obligations vis–à–vis du justiciable européen dès lors que l'exercice de la puissance publique est assuré par le service de renseignements d'un autre pays. La jurisprudence de la Cour confirme de manière constante que les pays signataires sont tenus de prendre des mesures positives pour protéger la vie privée afin que les personnes privées (!) ne violent pas l'article 8 de la convention, et ce y compris au plan horizontal où la personne ne se trouve pas face à la puissance publique mais à une autre personne[178]. Si un pays autorise un

---

[177] *Dimitri Yernault*, "Echelon" et l'Europe. La protection de la vie privée face à l'espionnage des communications, Journal des tribunaux, Droit européen 2000, 187 ss.

[178] CEDH, Abdulaziz, Cabales et Balkandali, 28.5.1985, p. 67; X et Y/Pays-Bas, 26.3.1985, p. 23; Gaskin –

service de renseignements étranger à intervenir sur son territoire, la protection nécessaire est d'autant plus grande que c'est dans ce cas une autre autorité qui exerce sa puissance. Il semble tout simplement logique de considérer que l'État doit veiller à la conformité des activités de services de renseignements avec les droits de l'homme sur son territoire.

8.4.2.2. Conséquences en ce qui concerne les stations

En Allemagne, les États–Unis d'Amérique disposent à Bad Aibling d'un territoire propre qu'ils utilisent exclusivement pour la réception d'émissions de satellites. À Menwith Hill, au Royaume-Uni, ils partagent un terrain dans le même but. Si un service de renseignements américain interceptait dans ces stations des communications non militaires de personnes privées ou d'entreprises en provenance d'un pays signataire de la convention, cela donnerait lieu à des obligations de contrôle. Dans la pratique, cela signifie que l'Allemagne et le Royaume–Uni, signataires de la convention, sont tenus de s'assurer que les activités des services de renseignements américains sont conformes aux droits fondamentaux. Cela s'impose d'autant plus que des représentants des ONG et de la presse ont déjà fait part à plusieurs reprises de leur inquiétude face aux agissements de la NSA.

8.4.2.3. Conséquences en ce qui concerne les écoutes pratiquées sur instructions de l'étranger

À Morwenstow, au Royaume–Uni, le GCHQ pratique en coopération avec la NSA, sur instructions de cette dernière, l'interception de communications civiles qui sont transmises telles quelles aux États–Unis. Même si les activités sont effectuées pour compte de tiers, il y a obligation de vérifier qu'elles sont conformes aux droits fondamentaux.

8.4.2.4. Obligation de vigilance par rapport aux pays tiers

S'agissant de pays signataires de la convention, on peut dans une certaine mesure considérer de part et d'autre que l'autre pays respecte aussi la convention. Cela n'est toutefois valable que jusqu'à ce qu'il soit établi qu'un pays signataire de la convention viole celle–ci de manière systématique et répétée. Les États–Unis ne sont pas signataires de la convention et ils ne se soumettent pas à un dispositif de contrôle comparable. Les activités de leurs services de renseignements sont très précisément réglementées, du moins par rapport aux citoyens des États–Unis, c'est–à–dire à des personnes qui se trouvent en séjour légal aux États–Unis. Les activités de la NSA à l'étranger font l'objet d'autres dispositions dont un grand nombre sont apparemment secrètes et donc inaccessibles. Préoccupant est en outre le fait que les services de renseignements américains sont soumis au contrôle des commissions de la Chambre des députés et du sénat, mais que les commissions parlementaires ne s'intéressent que très peu aux activités de la NSA à l'étranger.

Il apparaît donc opportun de lancer un appel à l'Allemagne et au Royaume–Uni pour qu'ils tiennent dûment compte des obligations qui découlent de la convention et qu'ils subordonnent l'autorisation d'activités de services de renseignements de la NSA sur leur territoire au respect de la convention dans ce contexte. À cet égard, trois aspects importants sont à prendre ne considération:

Royaume-Uni 7.7.1989, Z 38; Powell et Rayner, 21.2.1990, p. 41.

1) La convention prévoit que les atteintes à la vie privée ne sont possibles que sur la base de dispositions accessibles à tous et dont les conséquences sont prévisibles pour chacun. Il n'est satisfait à cette condition que si les États–Unis informent la population européenne sur les modalités de l'information. Aussi longtemps que la convention ne sera pas respectée, il faudra adapter les dispositions aux garanties offertes en Europe.

2) La convention prévoit que les interventions ne peuvent être disproportionnées et qu'il faut recourir aux moyens minimaux. Pour le citoyen européen, une intervention européenne est à considérer comme moins grave qu'une intervention américaine car dans le premier cas seulement il peut se tourner vers les voies de recours nationales[179]. Les interventions doivent donc dans la mesure du possible être effectuées par les Allemands ou par les Anglais, ce qui s'assortit logiquement dans les deux cas d'une possibilité de recours. Les Américains ont tenté à plusieurs reprises de justifier les écoutes en accusant les Européens de corruption[180]. Il a été rappelé aux Américains que tous les pays de l'UE disposent de systèmes pénaux en état de fonctionnement. En cas de suspicion, les États–Unis doivent s'en remettre au système pénal du pays d'accueil. S'il n'y a pas de suspicion, la surveillance est à considérer comme disproportionnée et donc contraire aux droits de l'homme, ce qui la rend inadmissible. La compatibilité avec la convention n'existe que si les États–Unis se limitent à des mesures de surveillance utiles à leur sécurité nationale, c'est–à–dire dépourvues de finalité pénale.

3) Comme il a déjà été indiqué, la jurisprudence de la Cour exige, pour qu'il y ait conformité aux droits fondamentaux, que des systèmes de contrôle et des garanties suffisantes contre les abus soient prévus. Cela signifie que la surveillance américaine des télécommunications sur le territoire européen n'est conforme aux droits de l'homme que si les États–Unis prévoient des contrôles efficaces dans les cas où ils interceptent des communications pour assurer leur sécurité nationale ou que les activités menées par la NSA sur le territoire européen soient soumises au contrôle du pays d'accueil (c'est-à-dire de l'Allemagne ou du Royaume-Uni).

C'est seulement à condition que ces trois exigences soient respectées qu'il sera possible de garantir que les écoutes de télécommunications pratiquées par les États-Unis sont conformes à la convention et que le niveau de protection garanti de manière uniforme en Europe par celle-ci est sauvegardé.

---

179 Cela assure aussi la conformité à l'article 13 de la convention des droits de l'homme qui reconnaît à la personne lésée le droit de s'adresser aux instances nationales.

180 *James Woolsey* (ancien directeur de la CIA), Why America Spies on its Allies, The Wall Street Journal Europe, 22.3.2000, 31 ders., Remarks at the Foreign Press Center, Transskript, 7.3.2000, http://cryptome.org/echelon-cia.htm.

9. Les citoyens de l'UE sont–ils suffisamment protégés face aux activités des services de renseignements?

9.1. Protection face aux activités des services de renseignements: rôle des parlements nationaux

Étant donné que les activités des services de renseignements pourraient à l'avenir constituer un aspect de la PESC, mais qu'il n'y a pour l'heure aucune disposition communautaire en la matière[181], l'organisation de la protection face aux activités des services de renseignements ne relève que des systèmes juridiques nationaux.

Dans ce contexte, les parlements nationaux jouent un double rôle: en tant que législateur, ils déterminent les effectifs et les pouvoirs des services de renseignements ainsi que l'organisation du contrôle de leurs activités. Comme il a été exposé au chapitre précédent, les parlements, lorsqu'ils abordent le problème de l'admissibilité de la surveillance des télécommunications, doivent s'en tenir aux limites fixées par l'article 8 de la convention: les dispositions doivent être nécessaires et proportionnelles et leurs conséquences doivent être prévisibles pour chacun. De plus, les pouvoirs des autorités de surveillance doivent être soumis à des mécanismes de contrôle appropriés et efficaces.

Par ailleurs, les parlements nationaux jouent dans la plupart des pays un rôle actif de contrôle. Le contrôle de l'exécutif (et donc des services de renseignements) est la deuxième fonction classique du parlement, à côté de la législation. Cela s'organise de diverses manières dans les États membres de l'UE, généralement des organes parlementaires coexistent avec des organes non parlementaires.

9.2. Pouvoirs des autorités nationales en matière de mesures de surveillance

La puissance publique peut prendre des mesures de surveillance dans un contexte pénal, pour préserver l'ordre ou pour assurer la sécurité de l'État (vis-à-vis de l'étranger)[182].

Dans le contexte pénal, le secret des communications peut être brisé dans tous les États membres dès lors qu'un soupçon fondé pèse sur l'auteur présumé d'une infraction pénale (lequel doit être dûment qualifié). Eu égard à la gravité de l'intervention, l'autorisation d'un magistrat est généralement requise[183]. La durée de la surveillance fait l'objet d'indications précises de même que le contrôle de celle–ci et la radiation des données.

Pour préserver la sécurité intérieure et l'ordre public, les possibilités d'interception sont étendues au-delà des recherches individuelles en cas de soupçon précis. Afin de dépister précocement les

---

181 Voir à ce propos également chapitre 7.

182 Ces objectifs sont reconnus comme justification d'atteinte à la vie privée par l'article 8, paragraphe 2, de la CEDH. Voir 8.3.2. ci–dessus.

183 À la différence du droit britannique qui confie la décision d'autorisation au Secretary of State (Regulation of Investigatory Powers Act 2000, Section 5 (1) und (3) (b).

mouvements extrémistes ou subversifs, le terrorisme ou la criminalité organisée, le législateur autorise la collecte d'informations concernant certaines personnes ou groupements. La collecte desdites informations et leur analyse sont effectuées par des services de renseignements intérieurs.

Enfin, la sécurité de l'État représente un aspect important des activités de surveillance. Le traitement, l'analyse et la présentation des informations via l'étranger incombent généralement à un service de renseignements à l'étranger[184]. Généralement, ce ne sont pas des individus précis qui sont les cibles de la surveillance mais plutôt des régions ou fréquences. En fonction des moyens dont dispose le service de renseignements, ainsi que de ses pouvoirs, l'éventail est vaste, qui va du renseignement radio à caractère militaire (ondes courtes) à la surveillance de tous les types de communications avec l'étranger. Dans nombre d'États membres, la surveillance des télécommunications à des fins de renseignements est interdite[185]. Dans d'autres, elle peut, dans certains cas, sous réserve de l'approbation d'une commission indépendante[186], être autorisée par un ministre[187] et ce sans restriction aucune pour de nombreux moyens de communication[188]. Les pouvoirs relativement importants de nombreux services de renseignements à l'étranger s'expliquent par le fait qu'ils assurent la surveillance des communications avec l'étranger, qui ne concernent qu'un faible pourcentage des justiciables, de sorte que ces activités suscitent peu d'intérêt.

9.3. Les contrôle des services de renseignements

Un contrôle efficace et global est d'autant plus important que, d'une part, les services de renseignements travaillent dans le secret, que leurs activités concernent le long terme, que les personnes concernées ignorent pendant longtemps ou (en fonction de la situation juridique) ne savent absolument rien de la surveillance effectuée et que, d'autre part, les activités de surveillance concernent dans bien des cas des groupes assez importants aux contours mal définis, de sorte que l'État peut obtenir à très bref délai un volume important de données à caractère personnel.

Tous les organes de contrôle – quelle que soit leur structure – sont évidemment confrontés au problème que, en raison du caractère particulier des services secrets, il est généralement très difficile de déterminer si toutes les informations ont été fournies ou si une partie de celles-ci ont été retenues. La réglementation doit donc se faire avec beaucoup de soin. En principe, on peut considérer que l'efficacité des contrôles et, partant, la garantie de la légalité des interventions, sont assurées dès lors que la possibilité d'ordonner une surveillance est l'apanage du niveau administratif le plus élevé, que sa réalisation nécessite l'autorisation préalable d'un magistrat et qu'un organe indépendant contrôle la réalisation des opérations. De plus, il est souhaitable, pour des raisons touchant à la démocratie et à l'état de droit, que les activités des services de renseignements dans leur ensemble soient conformes au principe de séparation des pouvoirs de

184 Pour l'activité des services de renseignement étranger, voir les commentaires détaillés du chapitre 2.

185 Autriche et Belgique.

186 En Allemagne, Gesetz zur Beschränkung des Brief-, Post-, und Fernmeldegeheimnisses (Gesetz zu Artikel 10 Grundgesetz). Conformément au § 9, la Commission doit être informée avant l'exécution (sauf risque de retard).

187 Au Royaume–Uni (Regulation of Investigatory Powers Act, Section 1) et en France (Art. 3 une 4 Loi 91-646 du 10 juillet 1991, loi relative au secret des correspondances émises par la voie des télécommunications).

188 En France (Art. 20 Loi 91-646 du 10 juillet 1991, loi relative au secret des correspondances émises par la voie des télécommunications).

contrôle d'un organe parlementaire.

Tel est le cas, dans une large mesure, en Allemagne. Dans ce pays, c'est le ministre fédéral compétent qui ordonne les activités de surveillance des télécommunications au niveau national. Sauf en cas d'urgence, une commission indépendante, non liée par un mandat (G 10-Kommission[189]) doit en être informée et c'est elle qui statue sur la nécessité et sur la recevabilité de l'intervention. Dans les cas où le service de renseignements à l'étranger est autorisé à pratiquer une surveillance de télécommunications en recourant au filtrage par clés de recherche, la commission statue également sur la recevabilité desdites clés. C'est à cette commission qu'incombe en outre le contrôle de la notification, prévue par la loi, à l'intéressé, ainsi que de la destruction des données recueillies par le BND.

Il existe en outre un organe de contrôle parlementaire (PKGr)[190] composé de neuf députés du Bundestag et qui est chargé de surveiller les activités des trois services de renseignements allemands. Cet organe a le droit de consulter les dossiers, d'entendre les agents des services de renseignements et de se rendre auprès de ces services ainsi que de se faire informer, ce qui ne peut être refusé que pour des raisons impératives d'accès à l'information ou pour des raisons de protection des droits de tiers ou lorsque la substance même de la responsabilité propre de l'exécutif est en jeu. Les travaux de cet organe sont secrets et ses membres sont tenus au devoir de réserve, même après avoir quitté l'organe en question. À mi–législature et à la fin de la législature, cet organe rend compte de ses activités de contrôle au Bundestag.

Ce contrôle des services de renseignements constitue cependant une exception parmi les États membres.

En France[191], seules les activités de surveillance nécessitant une table d'écoute requièrent l'autorisation du Premier ministre. Seules ces activités sont soumises à la surveillance d'une commission ad hoc (commission nationale de contrôle des interceptions de sécurité), qui se compose d'un député et d'un sénateur. L'autorisation d'une écoute demandée par un ministre ou par son délégué est soumise au président de la commission qui, en cas de doute quant à la légalité de l'opération, peut saisir la commission, qui émet des recommandations et, en cas de suspicion de violation de la loi susceptible de poursuites pénales, informe le ministère public. Les opérations d'écoute à des fins de défense des intérêts nationaux qui comportent l'interception de communications par radio ainsi que de communications par satellite ne sont soumises à aucune restriction et échappent donc au contrôle d'une commission.

Les activités des services de renseignements français ne sont par ailleurs pas soumises au contrôle d'une commission parlementaire spéciale, mais des travaux sont en cours à ce sujet. La

---

189 Pour des commentaires détaillés: Die Parlamentarische Kontrolle der Nachrichtendienste in Deutschland, Stand 9.9.2000, publié par le Deutscher Bundestag, Sekretariat des PKGr.

190 Gesetz über die Kontrolle nachrichtendienstlicher Tätigkeit des Bundes (PKGrG) du 17 juin 1999 BGBl I 1334 idgF.

191 Loi 91-646 du 10 juillet 1991, loi relative au secret des correspondances émises par la voie des télécommunications.

commission de la défense de l'Assemblée nationale a adopté une proposition[192], mais il n'y a pas encore eu de débat en séance à ce sujet.

Au Royaume-Uni, toute surveillance pratiquée sur le sol britannique nécessite l'autorisation d'un ministre (Secretary of State). Le texte de la loi n'indique toutefois pas clairement si l'"interception" non ciblée de communications soumises à l'épreuve des mots–clés relève de la notion d'interception utilisée dans la "Regulation of Investigatory Powers Act 2000" (RIP) dès lors que l'analyse n'est pas effectuée sur le sol britannique mais communiquée telle quelle à l'étranger, sans évaluation. Le contrôle du respect des dispositions de la RIP 2000 est effectué a posteriori par des "commissioners" (contrôleurs), des hauts magistrats en fonction ou retraités désignés par le Premier ministre. Le contrôleur chargé des écoutes (Interception Commissioner) contrôle l'octroi des autorisations d'écoute et suit l'examen des plaintes relatives aux écoutes. Le contrôleur responsable de l'Intelligence Service contrôle les autorisations concernant les activités des services de renseignements et de sécurité et suit les enquêtes relatives aux plaintes concernant ces services. L'Investigatory Powers Tribunal, présidé par un haut magistrat, examine toutes les plaintes relatives aux écoutes et aux activités des services.

Le contrôle parlementaire est assuré par l'Intelligence and Security Committee (ISC)[193], qui surveille les activités des trois services de renseignements civils (MI5, MI6 et GCHQ). Il est chargé notamment de contrôler les dépenses et la gestion ainsi que les activités du service de sécurité, du service de renseignements et du GCHQ. Cette commission se compose de neuf membres des deux Chambres mais ne peut compter aucun ministre en son sein. À la différence des commissions de contrôle d'autres pays, qui sont généralement élues ou désignées par le parlement ou par le président du parlement, celle-ci est nommée par le Premier ministre après consultation du chef de l'opposition.

Ces exemples montrent que les niveaux de protection sont très différents. S'agissant du contrôle parlementaire, le rapporteur tient à faire observer que l'existence de commissions chargées de surveiller les services de renseignements est très importante. Ces commissions présentent l'avantage de bénéficier de la confiance des services de renseignements parce que leurs membres sont tenus au secret et que leurs séances se déroulent à huis clos. De plus, ces commissions disposent de pouvoirs particuliers pour s'acquitter de leurs missions, ce qui est indispensable pour surveiller les activités menées dans le domaine secret.

Il convient de se féliciter de ce que la majorité des États membres de l'Union se sont dotés de commissions de contrôle parlementaires pour surveiller les services de renseignements. En Belgique[194], au Danemark[195], en Allemagne[196], en Italie[197], aux Pays–Bas[198] et au Portugal[199], il

---

192 Voir "Proposition de loi tendant à la création de délégations parlementaires pour le renseignement", et rapport afférent du député Arthur Paecht, Rapport fait au nom de la Commission de la défense nationale et des forces armées sur la proposition de loi (N° 1497) de M. Paul Quilès et plusieurs de ses collègues tendant à la création d'une délégation parlementaire pour les affaires de renseignement, enregistré`à la Présidence de l'Assemblée nationale le 23 novembre 1999.

193 Intelligence Services Act 1994, Section 10.

194 Comité permanent de contrôle des services de renseignements et de sécurité, Comité permanent R, Loi du 18 juillet 1991 /IV, organique du contrôle des services de police et de renseignements.

195 Udvalget vedrørende efterretningstjenesterne, Lov om etablering af et udvalg om forsvarets og politiets efterretningstjenester, lov 378 af 6/7/88.

196 Das parlamentarische Kontrollgremium (PKGr), Gesetz über die Kontrolle nachrichtendienstlicher Tätigkeit des Bundes (PKGrG)vom 17. Juni 1999 BGBl I 1334 idgF.

existe des commissions de contrôle parlementaires qui assurent à la fois le contrôle des services militaires et des services civils. Au Royaume–Uni[200], la commission de contrôle ne s'occupe que des services de renseignements civils (qui sont nettement plus importants), le service militaire étant contrôlé par la commission de la défense. En Autriche[201], les deux branches du service de renseignements sont contrôlées par deux commissions distinctes qui sont toutefois organisées de la même manière et qui bénéficient des mêmes droits. En Finlande[202] et en Suède[203] le contrôle parlementaire est assuré par un médiateur indépendant élu par le parlement. En France, en Grèce, en Irlande, au Luxembourg et en Espagne, il n'y a pas de commission parlementaire spécialisée. Le contrôle est assuré par les commissions dans le cadre des activités parlementaires général.

9.4. Analyse de la situation du citoyen européen

La situation du citoyen européen apparaît peu satisfaisante. L'ampleur des pouvoirs des services de renseignement en matière de surveillance des télécommunications présente des différences notables. La même remarque s'applique aux organes de contrôle. Tous les États membres qui possèdent un service de renseignements ne disposent pas d'organes de contrôle parlementaires indépendants dotés de pouvoirs de contrôle appropriés. On ne saurait parler d'un niveau de protection uniforme – tant s'en faut.

Du point de vue européen, cela est d'autant plus regrettable que cette situation n'affecte pas tellement les citoyens des États dont le comportement électoral peut influer sur le niveau de protection. Les effets défavorables concernent avant tout les ressortissants des autres États, puisque les activités des services de renseignements à l'étranger concernent par définition l'extérieur du pays. Le citoyen est relativement sans défense face aux systèmes étrangers. Le besoin de protection est donc plus grand encore dans ce domaine. Par ailleurs, il convient de ne pas perdre de vue qu'en raison du caractère particulier des services de renseignements, les citoyens de l'UE peuvent être concernés par les activités de plusieurs services de renseignements en même temps. Une protection uniforme conforme aux principes démocratiques serait souhaitable. Il conviendrait en outre d'examiner dans ce contexte si, en la matière, des dispositions communautaires relatives à la protection des données sont faisables.

Enfin, la question de la protection du citoyen européen se posera en des termes tout nouveaux lorsque, dans le cadre d'une politique de sécurité commune, la coopération entre services de

---

197 Comitato parlamentare, L. 24 ottobre 1977, n. 801, art. 11, Istituzione e ordinamento dei servizi per le informazioni e la sicurezza e disciplina del segreto di Stato.

198 Tweede-Kamercommissie voor de Inlichtingen- en Veiligheidsdiensten, 17. Reglement van orde van de Tweede Kamer der Staten-General, Art. 22.

199 Conselho de Fiscalização dos Serviços de Informações (CFSI), loi 30/84 du 5 septembre 1984, modifiée par la loi 4/95 du 21 février 1995, loi 15/96 du 30 avril 1996 et loi 75-A/97 du 22 juillet 1997.

200 Intelligence and Security Committee (ISC), intelligence services act 1994, Section 10.

201 Ständiger Unterausschuss des Landesverteidigungsausschusses zur Überprüfung von nachrichtendienstlichen Maßnahmen zur Sicherung der militärischen Landesverteidigung und dem Ständigen Unterausschuss des Ausschusses für innere Angelegenheiten zur Überprüfung von Maßnahmen zum Schutz der verfassungsmäßigen Einrichtungen und ihrer Handlungsfähigkeit, Art 52a B-VG, §§ 32b et ss. Geschäftsordnungsgesetz 1975.

202 Ombudsmann, base juridique pour le contrôle pour la police (SUPO): Poliisilaki 493/1995 §33 et Laki pakkokeinolain 5 a luvun muuttamisesta 366/1999 §15, pour l'armée: Poliisilaki 493/1995 §33 et Laki poliisin tehtävien suorittamisesta puolustusvoimissa 1251/1995 §5.

203 Rikspolisstyrelsens ledning, Förordning (1989:773) med instruktion för Rikspolisstyrelsen (règlement (1989:773) relatif à la police nationale).

renseignements des États membres deviendra réalité. Dans ce domaine, les institutions européennes seront appelées à adopter des dispositions de protection suffisantes. Il incombera au Parlement, champion du principe de l'État de droit, de faire en sorte qu'un contrôle approprié soit exercé par lui en tant qu'organe disposant d'une légitimité démocratique. Le Parlement devra en outre faire le nécessaire pour garantir le traitement confidentiel de données sensibles et autres documents secrets par une commission spéciale dont les membres seraient tenus au secret. Ce n'est que si ces conditions sont remplies qu'il sera réaliste de réclamer ces pouvoirs de contrôle en vue aussi d'assurer une bonne coopération entre les services de renseignements, coopération indispensable à une politique de sécurité commune digne de ce nom.

10. Protection contre l'espionnage économique

10.1. Économie et espionnage

On observe dans les entreprises économiques trois types d'informations. Premièrement, les informations qui font délibérément **l'objet d'une large diffusion**. Il s'agit d'informations objectives concernant les produits de l'entreprise (caractéristiques des produits, prix, etc.) et d'informations publicitaires qui influent sur l'image de l'entreprise.

Deuxièmement, il est des informations qui **ne sont ni protégées ni diffusées** parce qu'elles n'ont rien à voir avec la position concurrentielle de l'entreprise, par exemple la date de l'excursion d'entreprise, les menus de la cantine et la marque des télécopieurs utilisés.

Enfin, il y a les informations qui sont **mises à l'abri de l'accès de tiers**. Ces informations sont protégées de la concurrence mais aussi, si l'entreprise entend ne pas respecter la loi, de l'État (fisc, embargos, etc.). Différents niveaux de protection sont prévus qui vont jusqu'au secret absolu, par exemple pour les résultats de la recherche avant une demande de brevet ou la production de biens d'armement[204].

Dans le cas qui nous occupe, l'espionnage consiste à se procurer des informations tenues secrètes par une entreprise. Si le responsable est une entreprise concurrente, on parle d'**espionnage de concurrence** (espionnage industriel). S'il s'agit d'un service de renseignements d'État, on parle d'**espionnage économique**.

10.1.1. Les objectifs de l'espionnage

Les données stratégiques qui présentent un intérêt pour l'espionnage à caractère économique peuvent être classées suivant les branches et les services d'entreprise.

10.1.1.1. Branches

Il est évident que les informations des secteurs suivants présentent un grand intérêt: biotechnologie, génie génétique, technique médicale, technique environnementale, ordinateurs, logiciels, optoélectronique, stockage de données, céramique, etc.. La liste n'est pas exhaustive et elle se modifie constamment au rythme de l'évolution technique. Dans ces secteurs, l'espionnage consiste principalement à subtiliser des résultats de recherche ou à s'approprier des techniques de production particulières.

10.1.1.2. Départements d'entreprise

Les objectifs de l'espionnage se situent logiquement dans les services de recherche et de développement, d'achat, du personnel, de production, de distribution, de vente, de commercialisation, de produits et financiers. L'importance et la valeur de ces informations sont souvent sous–estimées (voir chapitre 10, point 10.1.4).

---

[204] Informationen für geheimschutzbetreute Unternehmen, Bundesministerium für Wirtschaft 1997.

10.1.2. Espionnage de concurrence

La position stratégique d'une entreprise sur le marché dépend de son statut dans les secteurs de la recherche et du développement, des procédés de fabrication, des lignes de produits, du financement, de la commercialisation, de la distribution, de l'achat et de la main–d'oeuvre[205]. Des informations concernant ces aspects présentent un grand intérêt pour tout concurrent parce qu'elles renseignent sur les projets et sur les points faibles d'une entreprise et permettent de prendre des contre–mesures stratégiques.

Une partie de ces informations sont accessibles au public. Il existe des entreprises de conseil très spécialisées qui, en toute légalité, effectuent des analyses de la concurrence, par exemple Roland & Berger en Allemagne. "Competitive Intelligence" est aujourd'hui un outil standard de gestion aux États–Unis[206]. À partir d'une multitude d'informations, il est possible de brosser le tableau clair d'une situation.

Le passage de la légalité à l'espionnage répréhensible dépend des moyens retenus pour se procurer les informations. On entre dans le domaine criminel dès lors que les moyens utilisés sont illicites. L'établissement d'analyses n'est pas répréhensible en soi. Les informations susceptibles d'intéresser un concurrent sont évidemment protégées et il n'est possible d'y accéder qu'en violant la loi. Les techniques utilisées ne se distinguent pas des méthodes d'espionnage évoquées au chapitre 2.

On ne dispose pas d'indications précises quant à l'ampleur de l'espionnage de concurrence. Comme pour l'espionnage classique, les chiffres occultes sont très élevés. Les deux parties concernées (auteur et victime) n'ont aucun intérêt à faire de la publicité. Pour les entreprises concernées, l'espionnage représente toujours une perte en terme d'image. Quant aux auteurs, ils n'ont aucun intérêt à ce que leurs activités soient mises au jour. Les cas qui sont soumis aux tribunaux sont donc très rares.

La presse fait pourtant sans cesse état de faits d'espionnage de concurrence. Le rapporteur a évoqué ce problème avec les responsables de la sécurité de grandes entreprises allemandes[207] et avec des dirigeants d'entreprises américaines et européennes. On peut dire en résumé que l'espionnage de concurrence, s'il est sans cesse constaté, n'influe pas sur la vie quotidienne des entreprises.

10.2. Les préjudices causés par l'espionnage

L'importance du chiffre occulte ne permet pas de chiffrer avec précision l'ampleur des dommages causés par l'espionnage de concurrence ou l'espionnage économique. À cela s'ajoute le fait que certains de ces chiffres sont volontairement gonflés. Les entreprises de sécurité et les services de contre–espionnage ont intérêt à situer l'ampleur du dommage dans la partie supérieure de l'échelle possible. Il n'empêche que les chiffres donnent une certaine idée.

---

205 *Michael E. Porter*, Competitive Strategy, Simon & Schuster (1998).
206 *Roman Hummelt*, Wirtschaftsspionage auf dem Datenhighway, Hanserverlag, 1997.
207 Détails et noms confidentiels.

Dès 1988, l'institut Max Planck évaluait le préjudice dû à l'espionnage économique en Allemagne à 8 milliards de marks au moins[208]. Le président de l'association des entreprises de conseil en sécurité d'Allemagne, Klaus-Dieter Matschke, avance, en s'appuyant sur l'avis d'experts, un chiffre de 15 milliards de marks par an. Le président des syndicats de police européens, Herman Lutz, chiffre le préjudice à 20 milliards de dollars par an. Le FBI[209] évoque pour les années 1992-1993 un préjudice de 1,7 milliard de dollars subi par l'économie américaine à cause de l'espionnage de concurrence et économique. L'ancien président de la commission de contrôle des services secrets de la Chambre des représentants des États–Unis parle de 100 milliards de dollars de préjudice lié aux commandes perdues et aux frais de recherche et développement supplémentaires. Entre 1990 et 1996, le phénomène a été à l'origine de la perte de 6 millions d'emplois[210].

En fait, il n'est pas nécessaire de connaître le préjudice avec précision. L'État est tenu de lutter contre l'espionnage de concurrence et économique en faisant appel aux services de police et de contre–espionnage indépendamment du montant du préjudice économique. Les chiffres globaux du préjudice ne peuvent servir de base non plus pour déterminer les décisions des entreprises relatives à la protection de l'information et aux mesures de lutte contre l'espionnage. Il appartient à chaque entreprise de calculer le préjudice maximal admissible, d'évaluer les possibilités d'intrusion et de comparer ces chiffres au coût de la sécurité. Le problème ne réside pas dans l'absence de chiffres globaux mais plutôt dans le fait que les grandes entreprises n'effectuent guère d'analyses coût-avantages, de sorte qu'elles négligent la sécurité.

10.3. Qui espionne?

Selon une étude de la société Ernest Young LLP[211], les principaux commanditaires sont les concurrents (39%), les clients (19%), les fournisseurs (9%) et les services secrets (7%). L'espionnage est le fait des propres collaborateurs de l'entreprise, d'officines spécialisées dans l'espionnage, de professionnels rémunérés ou d'agents des services secrets[212].

10.3.1. Collaborateurs de l'entreprise (délit d'initié)

Les ouvrages analysés, les indications des experts devant la commission et les entretiens du rapporteur avec des chefs de la sécurité et des services de contre–espionnage vont tous dans le même sens: le risque le plus grand vient de collaborateurs déçus ou insatisfaits. Faisant partie du personnel de l'entreprise, ils ont un accès direct à l'information, se laissent acheter et pillent les secrets d'entreprise pour leurs commanditaires.

Le risque est grand aussi en cas de changement d'emploi. Actuellement, il n'est pas nécessaire de copier des montagnes de papier pour emporter des informations importantes. Celles–ci peuvent être enregistrées discrètement sur disquette et remises au nouvel employeur lors du changement d'emploi.

---

208 IMPULSE, 3/97, pp.13 et ss.

209 *Louis J. Freeh*, Director FBI, Statement for the Record, Hearing on Economic Espionage, House Judiciary Committee, Subcommittee on Crime, Washington D.C., 9.5.1996.

210 *Robert Lyle*, Radio Liberty/Radio Free Europe, 10 février 1999.

211 Computerzeitung, 30.11.1995, p. 2.

212 *Roman Hummelt*, Spionage auf dem Datenhighway, Hanserverlag (1997) pp. 49 et suiv.

10.3.2. Officines spécialisées

Le nombre d'entreprises qui se sont spécialisées dans le pillage d'informations augmente sans cesse. Leurs agents sont en partie d'anciens collaborateurs de services de renseignements. Elles exercent souvent des activités de conseil en sécurité ou de recherche, fournissant des renseignements sur demande. Généralement, elles utilisent des méthodes légales, mais il en est qui recourent à des procédés illicites.

10.3.3. Hackers

Il s'agit de spécialistes de l'informatique qui, grâce à leurs connaissances, parviennent à accéder de l'extérieur aux réseaux informatiques. Initialement, il s'agissait de fous d'ordinateurs qui prenaient plaisir à venir à bout des mesures de sécurité des systèmes. Aujourd'hui, ils agissent sur commande, tant auprès des services que sur le marché.

10.3.4. Services de renseignements

La guerre froide ayant pris fin, les missions des services de renseignements ont évolué. La criminalité internationale organisée et l'économie constituent de nouveaux terrains d'activité (voir détails au chapitre 10, point 10.5).

10.4 Comment espionne–t–on?

D'après les informations fournies par les services de contre–espionnage et les responsables de la sécurité de grandes entreprises, l'espionnage économique a recours à toutes les méthodes et instruments du renseignement (voir point 2.4). Toutefois, les entreprises présentent des structures plus ouvertes que l'armée ou les services de renseignements ou encore les services gouvernementaux. Le domaine économique présente des risques supplémentaires:

- il est plus facile de trouver des collaborateurs parce que les possibilités offertes par la sécurité des entreprises ne sont pas comparables à celles des services de contre–espionnage;
- la mobilité de l'emploi fait que des informations importantes peuvent être emportées au moyen de l'ordinateur portable; le vol de tels appareils ou la copie discrète du disque dur après intrusion dans une chambre d'hôtel font partie des techniques habituelles de l'espionnage économique;
- l'intrusion dans les réseaux informatiques est plus facile que lorsqu'il s'agit d'organismes publics sensibles à la sécurité: les petites et moyennes entreprises ne sont pas sensibilisées aux problèmes de sécurité et prennent peu de précautions;
- les écoutes (voir point 3.2) sont elles aussi plus simples, pour les mêmes raisons.

L'analyse des informations recueillies fait ressortir que l'espionnage économique s'opère sur place ou sur le lieu de travail mobile parce que, à de rares exceptions près (voir chapitre 10, point 10.6), les informations recherchées ne peuvent être obtenues en interceptant les communications internationales.

10.5. Espionnage économique d'État

10.5.1. Espionnage économique stratégique effectué par les services de renseignements

La fin de la guerre froide a libéré des capacités de renseignements qui se sont investies plus qu'auparavant dans d'autres domaines. Les États–Unis ne cachent pas qu'une partie de leurs activités de renseignements concerne aussi l'économie. Cela englobe notamment le contrôle du respect des sanctions économiques, le contrôle du respect des conditions de livraison d'armes ou de biens à usage mixte, l'évolution des marchés des matières premières et celle des marchés financiers internationaux. D'après ce que le rapporteur a pu constater, les services américains ne sont pas les seuls à s'intéresser à ce domaine et cela ne fait pas l'objet d'une réprobation massive.

10.5.2. Les services de renseignements, agents de l'espionnage de concurrence

Ce qui suscite des critiques, c'est le fait que des services de renseignements soient mis à contribution pour procurer aux entreprises du pays des avantages dans la concurrence internationale. On distingue deux types de cas[213]:

10.5.2.1. Pays très avancés sur le plan technologique

Les pays très industrialisés peuvent profiter de l'espionnage industriel. En se renseignant sur l'état de développement d'un secteur, ils peuvent prendre des mesures (économie extérieure ou aide financière) qui améliorent la compétitivité de leur industrie ou leur permettent d'économiser des subventions. Un autre aspect important peut résider dans l'obtention de détails relatifs aux marchés à valeur élevée (voir chapitre 10, point 10.6).

10.5.2.2. Pays moins avancés sur le plan technique

Certains de ces pays sont confrontés aux problèmes de l'acquisition de savoir–faire technique, à l'effet de combler le retard qu'accusent leurs industries, et ce sans avoir à supporter de frais de développement et de redevances de licences. Ils doivent en outre se procurer des informations sur les produits et les techniques de fabrication afin de mettre sur le marché mondial, dans des conditions concurrentielles, des copies fabriquées à peu de frais (salaires). Il est établi que les services russes se sont vu confier cette tâche. La loi n° 5 de la Fédération de Russie relative aux renseignements étrangers mentionne l'acquisition d'informations économiques et technico–économiques parmi les missions des services de renseignements.

D'autres États (notamment Iran, Irak, Syrie, Libye, Corée du nord, Inde et Pakistan) ont à se procurer des informations pour leurs programmes nationaux d'armement, principalement dans le secteur nucléaire et dans celui des armes chimiques et biologiques. Un autre volet des activités des services de ces pays réside dans la gestion d'entreprises de couverture leur permettant d'acheter, sans éveiller les soupçons, des biens à usage mixte.

[213] Indication confidentielle d'un service de contre–espionnage, source protégée.

10.6. ECHELON est-il adapté à l'espionnage industriel?

Le contrôle stratégique des télécommunications internationales ne permet d'obtenir des informations utiles dans le contexte de l'espionnage de concurrence que par hasard. De fait, les informations sensibles se trouvent principalement dans les entreprises mêmes, **de sorte que l'espionnage de concurrence consiste à tenter de les obtenir par l'entremise de collaborateurs** ou de personnes infiltrées ou encore en pénétrant dans les réseaux informatiques. C'est seulement lorsque des données sensibles parviennent à l'extérieur par câble ou par voie hertzienne (satellite) qu'un système de surveillance peut être utilisé pour l'espionnage de concurrence. Cela se pratique systématiquement dans trois cas:

- pour les entreprises qui travaillent dans trois régions–horaires: les résultats intérimaires d'Europe sont envoyés en Amérique puis en Asie;
- dans le cas de vidéoconférences d'entreprises multinationales qui se déroulent grâce à des satellites ou à des liaisons câblées;
- lorsque des marchés importants sont négociés sur place (construction d'usines, infrastructures de télécommunications, construction de systèmes de transport, etc.), endroit à partir duquel il faut en référer à la maison–mère.

Si dans ces cas les entreprises ne protègent par leurs communications, l'interception de ces dernières fournit des données précieuses du point de vue de l'espionnage de concurrence.

10.7. Cas divulgués

On compte quelques cas d'espionnage économique ou de concurrence qui ont été évoqués dans la presse ou dans la littérature spécialisée. Une partie de ces sources ont été compulsées. On trouvera un résumé dans le tableau ci-après. Sont indiqués les participants, la date des faits, ce qui s'est passé, quel était l'objectif visé et quelles ont été les conséquences.

Il est à noter qu'une même affaire fait parfois l'objet de comptes rendus très divergents. Citons à titre d'exemple le cas Enercon: selon les sources, l'"auteur" est la NSA ou le ministère américain de l'économie ou encore la concurrence photographique.

Affaire	Qui	Quand	Les faits	Comment	Objectif	Conséquences	Source
Air France	DGSE	jusqu'en1994	Conversations d'hommes d'affaires en déplacement	Des micro-punaises ont été découverts dans les cabines de première classe d'Air France. La compagnie a fait des excuses publiques.	Collecte d'informations.	Non précisé.	„Wirtschaftsspionage: Was macht eigentlich die Konkurrenz?“ von Arno Schütze, 1/98
Airbus	NSA	1994	Informations relatives à un achat d'avions entre Airbus et la compagnie d'Arabie saoudite.	Interception de fax et de communications téléphoniques entre les partenaires.	Transmission des informations aux concurrents américains Boeing et McDonnell-Douglas.	Les Américains ont conclu un marché de 6 milliards de dollars.	„Antennen gedreht“, Wirtschaftswoche Nr.46 / 9. November 2000
Airbus	NSA	1994	Contrat de 6 milliards de dollars avec l'Arabie saoudite. Mise au jour d'une manœuvre de corruption du consortium européen Airbus.	Interception de fax et de communications téléphoniques entre le consortium Airbus et la compagnie le gouvernement d'Arabie saoudite par satellites de communication.	Mise au jour d'une manœuvre de corruption.	McDonnell-Douglas, le concurrent américain d'Airbus, a obtenu le marché.	Campbell in Stoa 1999, vol. 2/5, avec référence au Baltimore Sun, America's fortress of Spies, de Scott Shane et Tom Bowman, 3.12.1995, et au Washington Post, French Recent US Coups in New Espionnage, de William Drozdiak
BASF	Distributeur	non précisé	Description du procédé de fabrication de la matière première d'une crème dermatologique de l'entreprise BASF (département cosmétique)	Non précisé	Non précisé	Aucune car affaire éventée.	„Nicht gerade zimperlich“, Wirtschaftswoche Nr.43 / 16. Octobre 1992
Ministère fédéral de l'économie (Allemagne)	CIA	1997	Informations sur des produits de haute technologie au ministère fédéral de l'économie.	Intervention d'un agent.	Collecte d'informations.	L'agent a été démasqué et expulsé.	„Wirtschaftsspionage: Was macht eigentlich die Konkurrenz?“ von Arno Schütze, 1/98
Ministère fédéral de l'économie (Allemagne)	CIA	1997	Arrière-plan du processus Myconos de Berlin, crédits Hermès concernant les exportations vers l'Iran, structure d'entreprises allemandes fournissant des produits de haute technologie à l'Iran.	Un agent de la CIA se faisant passer pour un ambassadeur américain a mené des conversations amicales avec le chef pour la région arabe (principalement l'Iran) du service compétent du ministère fédéral de l'économie.	Collecte de renseignements.	Non précisé. Un fonctionnaire s'est adressé aux services de sécurité allemands, qui ont signalé aux Américains que l'opération de la CIA était inopportune. L'agent de la CIA a été rappelé.	„Wirtschaftsspionage. Die gewerbliche Wirtschaft im Visier fremder Nachrichtendienste“, Landesamt für Verfassungsschutz Baden-Württemberg, Stuttgart, Stand: 1998
Dasa	Renseignements russes	1996 – 1999	Vente et transfert de documents relatifs aux	2 Allemands en mission.	Collecte de renseignements sur les systèmes d'armes	SZ/30.5.2000:	„Anmerkungen zur Sicherheitslage der

Affaire	Qui	Quand	Les faits	Comment	Objectif	Conséquences	Source
			technologies d'armement d'une entreprise munichoise (d'après SZ/30.5.2000: Dasa à Ottobrunn)		(blindés et DCA).	Trahison "pas très grave" du point de vue militaire. Cela s'applique également au préjudice économique, constate le tribunal.	deutschen Wirtschaft“, ASW; Bonn, 2001 „Haftstrafe wegen Spionage für Russland“, 30 mai 2000
Embargo	BND	vers 1990	Reprise des exportations de technologies sous embargo à destination de la Libye (notamment Siemens).	Interception de télécommunications.	Mise au jour de transferts illégaux d'armes et de technologies.	Aucune conséquence particulière, les livraisons n'ont pas été interdites.	"Maulwürfe in Nadelstreifen", Andreas Förster, S. 110
Enercon	Experts en énergie éolienne d'Oldenburg et collaboratrice de Kenetech	Non précisé.	Éolienne de la société Enercon	Non précisé.	Non précisé.	Non précisé.	„Anmerkungen zur Sicherheitslage der deutschen Wirtschaft“, ASW; Bonn, avril 2001
Enercon	NSA	Non précisé.	Éolienne pour la production d'électricité développée par l'ingénieur A. Wobben	Non précisé.	Communication d'éléments techniques de Wobben à une entreprise américaine.	L'entreprise américaine demande le brevet avant Wobben (infraction au droit des brevets).	„Aktenkrieger“, SZ, 29. mars 2001
Enercon	Entreprise américaine Kenetech	1994	Détails importants d'une éolienne de haute technologie.	Photographies.	Demande de brevet couronnée de succès aux États-Unis.	Enercon GmbH a laissé tomber ses projets de conquête du marché américain.	„Sicherheit muss künftig zur Chefsache werden“, HB / 29 août 1996
Enercon	Ingénieur W. et entreprise américaine Kenetech	Mars 1994	Éolienne de type E-40 d'Enercon	L'ingénieur W. fournit des informations, une collaboratrice de Kenetech photographie l'installation et des détails.	Kenetech cherche des preuves pour une plainte pour infraction au droit des brevets contre Enercon pour collecte illicite d'informations touchant à des secrets d'entreprise. Selon un collaborateur de la NSA, ce qu'Enercon savait avait été communiqué à Kenetech par ECHELON.	Non précisé.	„Klettern für die Konkurrenz“, SZ 13. octobre 2000
Enercon	Kenetech Windpower	Avant 1996	Données relatives à une éolienne d'Enercon.	Des ingénieurs de Kenetech photographient le dispositif.	Reconstitution du système chez Kenetech.	Enercon obtient justice; action contre les espions; estimation de la perte: plusieurs centaines de millions de marks.	„Wirtschaftsspionage: Was macht eigentlich die Konkurrenz?“ von Arno Schütze, 1/98
Ministre du commerce du Japon	CIA	1996	Négociations relatives à des quotas d'importation de voitures américaines sur le	Piratage du système informatique du ministère japonais du commerce.	L'américain M. Kantor approuverait l'offre la plus basse.	Kantor accepte l'offre la plus basse.	„Wirtschaftsspionage: Was macht eigentlich die Konkurrenz?“ von Arno

Affaire	Qui	Quand	Les faits	Comment	Objectif	Conséquences	Source
			marché japonais.				Schütze, 1/98
Automobiles japonaises	Gouverne-ment américain	1995	Négociations concernant l'importation de véhicules de luxe japonais. Informations concernant les normes d'émission des voitures japonaises.	COMINT, sans précision.	Collecte de renseignements.	Non précisé.	Duncan Campbell in STOA 2/5 (1999) avec référence au Financial Post, Canada, 28.2.1998
López	NSA	Non précisé.	Vidéoconférence de VW et López	Interception à partir de Bad Aibling.	Transmission des informations à General Motors et à Opel.	L'interception aurait fourni au ministère public des indications très précises pour une enquête.	Bundeswehrhauptmann E. Schmidt-Eenboom, cité dans „Wenn Freunde spionieren“ www.zdf.msnbc.de/news/54637.asp?cp1=1
López	López et 3 de ses collabora-teurs	1992 - 1993	Documents et données des secteurs de la recherche, de la planification, de la fabrication et des achats (documents relatifs à une usine en Espagne, informations relatives au coût de différents modèles, études de projets, stratégies d'achat et d'économies).	Collecte de matériel.	Utilisation par VW des documents de General Motors.	Règlement à l'amiable entre les groupes. López démissionne de ses fonctions de directeur de VW. en 1996 verse 100 millions de dollars à GM/Opel (prétendus frais d'avocat) et achète durant 7 ans des pièces de rechange pour un total de 1 milliard de dollars.	„Wirtschaftsspionage. Die gewerbliche Wirtschaft im Visier fremder Nachrichtendienste“, Landesamt für Verfassungsschutz Baden-Württemberg, Stuttgart, Stand: 1998
López	NSA	1993	Vidéoconférence entre López et le directeur de VW F. Piëch	Extrait de vidéoconférence et communication à GM.	Protection des secrets de l'entreprise américaine GM que López entendait communiquer à VW (tarifs, projets secrets relatifs à une nouvelle usine et à un nouveau véhicule).	López est démasqué, l'action en justice est suspendue en 1998 moyennant versement d'amendes. Rien au sujet de NSA.	„Antennen gedreht“, Wirtschaftswoche Nr.46 / 9. novembre 2000 „Abgehört“, Berliner Zeitung, 22 janvier 1996 „Die Affäre López ist beendet“, Wirtschaftsspiegel, 28 juillet 1998 „Wirtschaftsspionage: Was macht eigentlich die Konkurrenz?“ von Arno Schütze, 1/98
Los Alamos	Israel	1988	Deux collaborateurs du programme israélien de recherche nucléaire forcent	Piratage.	Collecte de renseignements sur de nouveaux détonateurs nucléaires américains.	Aucune conséquence particulière; les pirates s'enfuient en Israël; l'un d'entre	"Maulwürfe in Nadelstreifen", Andreas Förster, p. 137

Affaire	Qui	Quand	Les faits	Comment	Objectif	Conséquences	Source
			l'ordinateur central du laboratoire nucléaire de Los Alamos.			eux est arrêté mais aucun lien avec les services secrets israéliens n'est officiellement évoqué.	
Contrebande	BND	Années 70	Contrebande d'installations informatiques en RDA.	Non précisé.	Mise au jour de transferts de technologies à destination du bloc de l'Est.	Pas de conséquences particulières, les livraisons ne sont pas interdites.	"Maulwürfe in Nadelstreifen", Andreas Förster, p. 113
TGV	DGSE	1993	Calcul des coûts de Siemens. Commande pour la livraison de trains à grande vitesse destinés à la Corée du Sud.	Non précisé.	Offre inférieure.	Le constructeur ICE perd le marché au profit d'Alcatel-Alsthom	„Wirtschaftsspionage: Was macht eigentlich die Konkurrenz?“ von Arno Schütze, 1/98
TGV	Non précisé.	1993	Calcul des coûts d'AEG et de Siemens concernant un marché public en Corée du Sud concernant la fourniture de trains à grande vitesse.	Siemens dénonce une interception de ses communications téléphoniques et par fax dans son établissement de Séoul.	Avantage pour le concurrent anglo-français GEC-Alsthom.	GEC-Alsthom est retenu alors que l'offre allemande était plus favorable.	„Abgehört“, Berliner Zeitung, 22 janvier 1996
Thomson-Alcatel contre Raytheon	CIA/ NSA	1994	Passation d'un marché brésilien relatif à la surveillance par satellite de l'Amazone à la firme française Thomson-Alcatel (1,4 milliard de dollars).	Interception des communications du soumissionnaire retenu (Thomson-Alcatel).	Mise au jour d'une opération de corruption.	Clinton se plaint auprès du gouvernement brésilien; sous la pression du gouvernement des États-Unis, le marché est réattribué à l'entreprise américaine Raytheon.	"Maulwürfe in Nadelstreifen", Andreas Förster, p. 91
Thomson-Alcatel contre Raytheon	Ministère américain de l'économie	1994	Négociations relatives à un projet de surveillance par radar de la forêt tropicale brésilienne.	Non précisé.	Obtention du marché.	Les groupes français Thomson CSF et Alcatel perdent le marché au profit de l'entreprise américaine Raytheon.	„Antennen gedreht“, Wirtschaftswoche Nr.46 / 9 novembre 2000
Thomson-Alcatel contre Raytheon	NSA Ministère du commerce		Négociations relatives à un projet (1,4 milliard de dollars) relatif à la surveillance de l'Amazone. Mise au jour d'une opération de corruption du groupe de sélection brésilien. Remarque de Campbell: Rayethon équipe une station d'interception à Sugar Grove.	Interception des négociations entre Thomson CSF et le Brésil et communication à Raytheon.	Mise au jour d'une affaire de corruption; obtention du marché.	Raytheon obtient le marché.	Duncan Campbell in STOA 2/5 de 1999 avec référence au New-York Times, How Washington Inc makes a sale de David Sanger, 19.2.1995 et http://www:rayethon:com/sivam/contract:html
Thyssen	BP	1990	Marché (plusieurs millions) relatif à l'exploitation de gaz et de pétrole en mer du Nord.	Interception de fax du soumissionnaire retenu (Thyssen).	Mise au jour d'une affaire de corruption.	BP réclame des dommages-intérêts à Thyssen.	"Maulwürfe in Nadelstreifen", Andreas Förster, p. 92
VW	Non précisé.	„années passées“	Non précisé.	Caméra infrarouge enterrée et transmettant ses images par voie hertzienne.	Collecte de renseignements sur les innovations.	VW annonce des pertes considérables.	„Sicherheit muss künftig zur Chefsache werden“, HB / 29. août 1996
VW	Non précisé.	1996	Circuit d'essais de VW (Ehra-Lessien).	Caméra cachée.	Informations concernant les nouveaux modèles de VW.	Non précisé.	„Auf Schritt und Tritt“ Wirtschaftswoche Nr. 25,

Affaire	Qui	Quand	Les faits	Comment	Objectif	Conséquences	Source
							11 juin 1998

10.8. Protection contre l'espionnage économique

10.8.1. Protection juridique

Les systèmes juridiques des pays industrialisés punissent le vol de secrets d'entreprise. Comme dans tous les autres domaines du droit pénal, les niveaux de protection nationaux sont différents. En règle générale, les sanctions sont nettement moins sévères que dans les cas d'espionnage en rapport avec la sécurité militaire. Dans nombre de cas, l'espionnage de concurrence n'est interdit que s'il concerne des entreprises du pays, pas s'il concerne des entreprises de l'étranger. Tel est également le cas aux États-Unis.

La législation afférente n'interdit essentiellement que l'espionnage entre entreprises. Il est douteux qu'elle restreigne aussi les activités des services de renseignements nationaux. En effet, les dispositions qui ont créé ceux-ci les autorisent à s'emparer des informations.

Un cas limite se présente lorsqu'un service de renseignements obtient par espionnage des informations qu'il met à la disposition de différentes entreprises. Normalement, ce cas n'est plus couvert par les dispositions qui donnent des pouvoirs spéciaux aux services de renseignements. Au sein de l'UE, il s'agirait là d'une infraction au traité CE.

Abstraction faite de cela, il serait très difficile à une entreprise, dans la pratique, de s'adresser aux tribunaux. L'interception ne laisse pas de trace, c'est-à-dire pas de preuve utilisable en justice.

10.8.2. Autres entraves à l'espionnage économique

Les différents pays acceptent le fait que les services de renseignements, dans la recherche d'informations stratégiques, exercent aussi leurs activités dans le domaine économique. Toutefois, il est largement porté atteinte à ce "gentleman's agreement" en cas d'espionnage de concurrence au profit des industries nationales. Si un pays est pris la main dans le sac, il se trouve confronté à de gros problèmes politiques. Cela s'applique aussi à une puissance mondiale telle que les États-Unis, qui verraient leurs prétentions au leadership politique mondial gravement compromises. Les puissances moyennes pourraient se permettre cela, mais pas une puissance mondiale.

À côté des problèmes politiques, se pose la question pratique de savoir à quelle entreprise communiquer les résultats de l'espionnage de concurrence. Dans le secteur de la construction aéronautique, la réponse est facile parce qu'il n'y a que deux grands fournisseurs au monde. Dans tous les autres cas, les fournisseurs sont nombreux et ils ne sont pas propriété de l'État, ce qui rend difficile d'en favoriser un. S'agissant de la communication d'informations relatives aux offres de concurrents dans le contexte de marchés publics internationaux, la communication à tous les concurrents du pays serait concevable. Tel est notamment le cas lorsqu'il existe une structure gouvernementale de soutien accessible à tous les concurrents du pays - ce qui est le cas aux États-Unis (Advocacy Center). En cas de vol de technologie débouchant sur une demande de brevet, l'égalité de traitement des entreprises devient

impossible.

Cela poserait un grave problème dans le système politique américain. Les hommes politiques américains sont largement tributaires, pour le financement de leurs campagnes électorales, des dons des entreprises de leur circonscription. Si un cas de favoritisme des services de renseignements à l'égard d'une entreprise était divulgué, il y aurait des remous considérables dans le système politique. Pour reprendre la formule de l'ancien directeur de la CIA Woolsey, lors d'un entretien avec les représentants de la commission: "In this case the hill (i.e. the US-Congress) would go mad!" ("Dans ce cas, le Congrès deviendrait enragé!"). À n'en pas douter!

10.9. Les États–Unis et l'économie après la guerre froide

Depuis 1990, le gouvernement américain tend de plus en plus à mettre sur le même plan la sécurité économique et la sécurité nationale. Le rapport annuel de la Maison blanche "National Security Strategy"[214] ne cesse de souligner que **la sécurité économique fait partie intégrante non seulement des intérêts nationaux mais aussi de la sécurité nationale**.

À l'origine de cette évolution, il y a plusieurs causes. En fait, trois facteurs ont contribué à ce qu'elle ait lieu:

– l'intérêt que les services de renseignement attachent à une mission se poursuivant après la guerre froide,

– la simple reconnaissance par le ministère américain des affaires étrangères que désormais, le rôle dirigeant des États-Unis dans le monde, la guerre froide ayant pris fin, doit se fonder non pas uniquement sur la force militaire mais aussi sur la puissance économique,

– l'intérêt attaché, en politique intérieure, par le Président Clinton, au renforcement de l'économie américaine et à la création d'emplois.

[214] Stratégie de sécurité nationale.

Cette convergence d'intérêts de l'administration américaine a eu des conséquences pratiques.

En toute logique, le FBI a, depuis 1992, concentré ses activités de contre-espionnage sur l'espionnage économique et lancé en 1994 un "Economic Counterintelligence Program", qui est, selon Freeh, directeur du FBI, devant le Parlement, un programme **défensif**. Ce programme doit empêcher que la compétitivité de l'économie américaine soit mise en danger par le vol d'informations.

Logiquement, du moins dans l'optique américaine, le gouvernement a fait appel à la CIA et, par la suite, à la NSA pour lutter contre les distorsions de concurrence par la corruption. James Woolsey, ancien directeur de la CIA, n'a laissé plané aucun doute à ce propos lors d'une conférence de presse qu'il a donnée le 7 mars 2000 à la demande du ministère américain des affaires étrangères[215].

Logiquement, le ministère américain du commerce a organisé ses activité de promotion des exportations de telle façon qu'une entreprise américaine ne se trouve en face que d'un seul interlocuteur lorsqu'elle veut exporter. En l'occurrence, toutes les possibilités du gouvernement ont été concentrées dans une perspecitve non seulement passive mais aussi active (pour plus de détails à ce propos, voir chapitre 10, point 10.9.4.).

10.9.1. Le défi pour le gouvernement américain: l'espionnage économique contre les entreprises américaines

Les actions de renseignement visant l'économie américaine ne sont ni inhabituelles ni nouvelles. Les États-Unis, comme d'autres grandes nations industrielles, ont été pendant des dizaines d'années la cible de l'espionnage économique. Toutefois, pendant la guerre froide, l'obtention d'informations économiques et technologiques n'était qu'une activité corollaire de l'espionnage classique. Après la fin de la guerre froide, l'espionnage économique est devenu un objectif en soi[216] .

[215] State Department Foreign Press Center Briefing, Subject: Intelligence Gathering and Democracies: The Issue of Economic and Industrial Espionage, Washington DC, 7.3.2000

[216] Statement for the Record of *Louis J. Freeh*, Director FBI, Hearing on Economic Espionage, House Judiciary Committee, Subcommittee on Crime, Washington DC, 9.5.1996

Louis J. Freeh, directeur du FBI, a expliqué en 1996 dans le détail, devant le Congrès que l'économie américaine était la cible de l'espionnage économique auquel se livraient des services de renseignement d'autres pays. Il a dit, mot pour mot, que des gouvernements étrangers prenaient pour cible – et ce par différents moyens – des personnes, des firmes, des industries et le gouvernement américain lui-même pour voler ou obtenir de façon illicite des technologies, données et informations critiques, afin de procurer des avantages concurrentiels à leur propre industrie[217]. Il n'empêche que le vol d'informations par les Américains progresse également de la même façon. Les autres déclarations faites par le directeur Freeh devant le parlement américain sont résumées ci-après. Votre rapporteur déplore ici que le gouvernement américain n'ait pas autorisé une délégation de la commission à s'entretenir de ces questions avec le FBI, ce qui aurait permis d'actualiser les informations. Aussi votre rapporteur part-il du principe que dans l'esprit du gouvernement américain, l'audition devant la Chambre des représentants en 1996 reflète l'état actuel de la menace que représente l'espionnage économique pour l'économie américaine, et se réfère-t-il à cette source.

10.9.1.1. Les acteurs

Au moment de l'audition, le FBI enquêtait sur des personnes ou des organisations de 23 pays soupçonnées d'espionnage écnomique contre les États-Unis. Si certains opposants idéologiques ou militaires des États-Unis poursuivent purement et simplement leurs activités du temps de la guerre froide[218], d'autres gouvernements pratiquent un espionnage économique et technologique, alors qu'ils sont depuis longtemps des alliés militaires et politiques des États-Unis. En l'occurrence, ils profitent souvent de leurs facilités d'accès aux informations américaines. Certains d'entre eux ont développé une infrastructure propre pour exploiter les informations concernant les technologies de pointe et les utiliser dans la concurrence avec les entreprises américaines. Concrètement, aucun pays n'est cité, ce qui n'empêche qu'il est question, en termes voilés, de la Russie, d'Israël et de la France[219].

10.9.1.2. Objectifs de l'espionnage économique

Les objectifs de l'espionnage économique que cite le FBI correspondent à ce qui est dit au chapitre 10, point 10.1.1. Toutefois, la haute technologie et l'industrie de la défense sont citées en tant qu'objectifs prioritaires. Il est intéressant de constater que sont mentionnées en tant qu'objectifs de l'espionnage économique poursuivis de façon **agressive** les informations sur des offres, des contrats, des clients et l'information stratégique dans ces secteurs[220].

---

[217] „Consequently foreign governments, through a variety of means, actively target U.S. persons, firms, industries and the U.S. government itself, to steal or wrongfully obtain critical technologies, data and information in order to provide their own industrial sectors with a competitive advantage.".

[218] „The end of the Cold War has not resulted in a peace dividend regarding economic espionage“, *Freeh*, Statement for the Record of *Louis J. Freeh*, Director FBI, Hearing on Economic Espionage, House Judiciary Committee, Subcommittee on Crime, Washington DC, 9.5.1996 .

[219] Interprétation par votre rapporteur des déclarations évasives faites par *Louis J. Freeh* devant la commission.

[220] En la matière, l'interception des communications est une méthode pleine de promesses!

10.9.1.3. Méthodes

Dans le cadre de l'Economic Counterintelligence Program, le FBI a conçu une série de méthodes d'espionnage. La plupart du temps, différentes méthodes sont utilisées ensemble, et ce n'est que rarement qu'une seule méthode est utilisée. Le FBI convient que la meilleure source est une personne dans une entreprise ou une organisation, ce qui, en règle générale, vaut également pour des contextes autres qu'américains (cf. chapitre 10, points 10.3 et 10.4). Lors de l'audition, le FBI a fait état de l'utilisation de personnes aux fins de l'espionnage, ne disant mot – ce qui est étonnant – des méthodes électroniques.

10.9.2. Attitude du gouvernement américain face à l'espionnage économique actif

L'ancien directeur de la CIA Woolsey a, lors d'une conférence de presse [221] et d'un entretien avec des membres de la commission à Washington, résumé comme suit l'activité d'interception du service secret américain:

1. les États-Unis surveillent les communications internationales afin de se procurer des informations générales sur l'évolution économique, sur les livraisons de biens à usage mixte et sur le respect des embargos,
2. les États-Unis surveillent spécialement les communications d'entreprises dans le contexte de la passation de marchés afin d'empêcher les distorsions liées à la corruption au détriment des entreprises américaines. Interrogé à ce propos, Woolsey n'a cité aucun exemple concret.

La corruption est interdite aux entreprises américaines et les responsables du contrôle sont tenus de signaler les versements de pots de vin. Si la surveillance des communications permet de constater des affaires de corruption dans les marchés publics, l'ambassadeur des États-Unis intervient auprès du gouvernement du pays concerné. Les entreprises américaines concurrentes ne sont en revanche pas informées directement. Il a exclu de façon catégorique tout espionnage de concurrence pur et simple.

George J. Tenet, directeur de la CIA, s'est exprimé dans le même sens à l'occasion d'une audition devant la commission de contrôle des services secrets de la Chambre des représentants le 12 avril 2000[222]: les États-Unis n'ont ni pour politique ni pour pratique de se livrer à des activités d'espionnage pour procurer un avantage déloyal aux entreprises américaines. Au cours de la même audition, Tenet a également expliqué que lorsqu'il s'agit d'informations portant sur la corruption, ces informations sont transmises à d'autres services gouvernementaux, afin que ceux-ci puissent aider les entreprises américaines[223]. En réponse à

---

[221] *James Woolsey*, Remarks at the Foreign Press Center, Transskript, 7.3.2000, http://cryptome.org/echelon-cia.htm

[222] „It is not the policy nor the practice of the U.S. to engage in espionage that would provide an unfair advantage to U.S. Companies“

[223] „As I indicated also in my testimony, there are instances where we learn, that foreign companies or their governments bribe, lie, cheat or steal their way to disenfranchise American companies. When we generate this information, we take it to other appropriate agencies, make them aware of it. They use that information through other means and channels to see if they can assist an American company. But we play defense, we never play offense, and we never will play offense.”

une question du député Gibbons, Tenet a reconnu que l'espionnage de concurrence n'était pas interdit par la loi, faisant toutefois observer qu'il ne voyait pas la nécessité d'une telle interdiction, dès lors que les services ne se livreraient pas à ce genre d'activités.

Porter Goss, président de la commission du contrôle des services secrets de la Chambre des représentants, a, lors d'un entretien qu'il a accordé à Washington, décrit de la même façon les activités d'interception.

10.9.3. Situation juridique en matière de corruption d'agents publics[224]

La corruption aux fins de s'assurer des marchés n'est pas un phénomène européen mais bien mondial. Selon le Bribe Payers Index (BPI), publié en 1999 par Transparency International, qui classe les 19 principaux pays exportateurs selon leur propension à offrir des pots-de-vin, l'Allemagne et les États-Unis se partagent la neuvième place. La pratique de la corruption est jugée moindre dans le cas de la Suède, de l'Autriche, des Pays-Bas, du Royaume-Uni et de la Belgique. Seules l'Espagne, la France et l'Italie sont plus mal placées[225].

Pour justifier l'espionnage économique, les Américains invoquent les pratiques de corruption des entreprises européennes. Cette approche est contestable non seulement parce que des comportements impropres isolés ne sauraient être un motif justifiant un espionnage général mais aussi et surtout parce que de telles pratiques s'apparentant à la loi du plus fort ne seraient tolérables que dans un environnement échappant au droit.

En Europe, la corruption est réprimée par la loi avec la même rigueur qu'aux États-Unis. La similitude des intérêts a conduit à l'adoption, en 1997, de la Convention de l'OCDE sur la lutte contre la corruption d'agents publics étrangers dans les transactions commerciales internationales[226]. Cette convention oblige les États signataires à réprimer la corruption d'un agent public étranger et comporte, outre la définition du fait générateur du délit, des dispositions concernant les sanctions, la juridiction et l'exécution.

La Convention, qui est entrée en vigueur le 15 février 1999, a été transposée et ratifiée par tous les États membres de l'Union européenne, à l'exception de l'Irlande. Les États-Unis ont transposé la Convention par l'International Anti-Bribery and Fair Competition Act de 1998[227] qui a adapté leur Foreign Corrupt Practices Act (FCPA) de 1977, qui fait obligation aux entreprises de tenir une comptabilité et qui interdit la corruption d'agents publics étrangers.

---

[224] *Albin Eser, Michael Überhofer, Barbara Huber* (Eds), Korruptionsbekämpfung durch Strafrecht. Ein rechtsvergleichendes Gutachten zu den Bestechungsdelikten im Auftrag des Bayerischen Staatsministeriums der Justiz, edition iuscrim (1997)

[225] L'échelle va de 10 (taux de corruption bas) à 0 (taux de corruption élevé): Suède (8,3), Australie (8,1), Canada (8,1), Autriche (7,8), Suisse (7,7), Pays-Bas (7,4), Royaume-Uni (7,2) Belgique (6,8), Allemagne (6,2), États-Unis (6,2), Singapour (5,7), Espagne (5,3), France (5,2), Japon (5,1), Malaisie (3,9), Italie (3,7), Taïwan (3,5), Corée du Sud (3,4), Chine (3,1).

http://www.transparency.org/documents/cpi/index.html#bpi

[226] Convention sur la lutte contre la corruption d'agents publics étrangers dans les transactions commerciales internationales

http://www.oecd.org/daf/nocorruption/20nov1e.htm

[227] OFFICE OF THE CHIEF COUNSEL FOR INTERNATIONAL COMMERCE, Legal Aspects of International Trade and Investment, http://www.ita.doc.gov/legal/

Pas plus aux États-Unis que dans les États membres de l'Union européenne, les pots-de-vin payés aux agents publics étrangers ne sont regardés comme des charges déductibles[228].

Alors que la convention de l'OCDE ne vise que la lutte contre la corruption d'agents publics étrangers, le Conseil de l'Europe a adopté en 1999 deux conventions plus ambitieuses, qui ne sont toutefois pas encore entrées en vigueur. La convention pénale en matière de corruption[229] vise également la corruption dans le secteur privé. Si elle a été signée par tous les États membres de l'Union européenne, exception faite de l'Espagne, ainsi que par les États-Unis, elle n'a toutefois été ratifiée que par le Danemark.

La convention civile en matière de corruption[230] arrête des règles dans le domaine de la responsabilité et de la réparation du préjudice, déclarant notamment nuls et non avenus les contrats et clauses contractuelles imposant le paiement de pots-de-vin. Elle a été signée par tous les États membres de l'Union européenne, hormis les Pays-Bas, le Portugal et l'Espagne. Les États-Unis ne l'ont pas signée.

Dans le cadre de l'Union européenne également, ont été adoptés deux actes concernant la lutte contre la corruption, à savoir la convention relative à la lutte contre la corruption impliquant des fonctionnaires et l'action commune relative à la corruption dans le secteur privé.

La convention relative à la lutte contre la corruption impliquant des fonctionnaires des Communautés européennes ou des fonctionnaires des États membres de l'Union européenne[231] a pour but de garantir que sont érigées en infractions pénales dans toute l'Union européenne la corruption passive et la corruption active de fonctionnaires. Les États membres sont tenus de sanctionner la corruption passive et la corruption active des fonctionnaires, qu'il s'agisse de l'un de leurs fonctionnaires, d'un fonctionnaire d'un autre État membre ou d'un fonctionnaire communautaire.

Par l'action commune relative à la corruption dans le secteur privé[232], il est garanti que la corruption passive et la corruption active d'entreprises sont érigées en infractions pénales. En l'occurrence, des sanctions pénales sont prévues non seulement pour les personnes physiques mais aussi pour les personnes morales. Le champ d'application de l'action commune est cependant plus limité que celui de la convention relative à la lutte contre la corruption impliquant des fonctionnaires, dans la mesure où les États membres sont tenus uniquement de sanctionner des faits commis au moins en partie sur leur territoire. Il appartient aux États membres de décider eux-mêmes si l'application des sanctions peut être étendue aux infractions commises à l'étranger par leurs propres ressortissants ou en faveur de personnes morales locales. L'Allemagne et l'Autriche ont érigé en infractions pénales les délits de

---

[228] http://www.oecd.org/daf/nocorruption/annex3.htm

[229] Criminal Law Convention on Corruption, http://conventions.coe.int/treaty/EN/WhatYouWant.asp?NT=173&CM=8&DF=21/06/01

[230] Civil Law Convention on Corruption ETS no.: 174, http://conventions.coe.int/treaty/EN/WhatYouWant.asp?NT=174&CM=8&DF=21/06/01

[231] Convention établie sur la base de l'article K.3, paragraphe 2, point c) du traité sur l'Union européenne, relative à la lutte contre la corruption impliquant des fonctionnaires des Communautés européennes ou des fonctionnaires des États membres de l'Union européenne, JO C 195 du 25.6.1997, p. 2.

[232] Action commune du 22 décembre 1998, adoptée par le Conseil sur la base de l'article K.3 du traité sur l'Union européenne, relative à la corruption dans le secteur privé (98/742/JAI), JO L 358 du 31.12.1998, p. 2.

corruption commis à l'étranger dès lors que ceux-ci sont également punissables sur le territoire où ils ont été commis.

10.9.4. Rôle de l'Advocacy Center dans la promotion des exportations américaines

Par l'Executive Order 12870, le Président Clinton a constitué en 1993 le Trade Promotion Coordinating Committee (TPCC)[233]. Celui-ci doit coordonner le développement de la politique de promotion commerciale du gouvernement américain et concevoir une stratégie à cet effet. En vertu de l'Executive Order, un représentant du National Security Council (NSC)[234] fait également partie du TPCC. Le NSC définit la politique de sécurité nationale des États-Unis en ce qui concerne tant les questions de politique intérieure, de politique étrangère et de politique militaire que les tâches des services de renseignement. Les priorités d'action du NSC se modifient en fonction des priorités fixées par le Président. Le 21 janvier 1993, le Président Clinton a élargi le NSC par le PDD2 et conféré dans le même temps davantage de poids aux questions économiques dans la formulation de la politique de sécurité. Font notamment partie du NSC le Président, le vice-président, le ministre des affaires étrangères et le ministre de la défense. Le Directeur de la CIA est membre à titre consultatif.

10.9.4.1. Missions de l'Advocacy Center

L'Advocacy Center, implanté au ministère américain du commerce, est l'élément clé de la stratégie d'exportations menée par Clinton et poursuivie par Bush. Il représente le point de contact entre le TPCC et l'économie américaine. Créé en 1993, ce centre a, selon ses propres dires, aidé des centaines d'entreprises américaines à obtenir des marchés publics à l'étranger.

L'Advocacy Center[235] aide les entreprises américaines:

– en mobilisant l'ensemble des moyens à la disposition du gouvernement américain: experts financiers et réglementaires par pays et secteur, réseau mondial des agents commerciaux, Maison blanche,
– en s'employant à homogénéiser les règles et à promouvoir une concurrence ouverte pour les appels d'offres internationaux, depuis les projets d'infrastructure portant sur plusieurs milliards de dollars jusqu'au contrat stratégique pour une petite entreprise,
– en menant des négociations au nom des entreprises américaines depuis le début jusqu'à la fin, par la voie d'un support concret,
– en soutenant l'emploi américain et en promouvant les exportations américaines en faisant en sorte que les entreprises américaines puissent s'assurer des projets et contrats outre-mer,

– en aidant les entreprises américaines confrontées à des négociations dans l'impasse par suite de l'inaction ou de la bureaucratie de gouvernements étrangers.

[233] Archives de la Maison blanche, http://govinfo.library.unt.edu/npr/library/direct/orders/tradepromotion.html.

[234] Page d'accueil du National Security Council (NSC), http://www.whitehouse.gov/nsc.

[235] Brochure du TPCC concernant l'Advocacy Center, octobre 1996.

10.9.4.2. Méthodes de travail[236]

Le centre n'occupe qu'un directeur et une petite équipe de 12 personnes (situation à la date du 6.2.2001). Les secteurs d'activité des responsables de projets sont la Russie et les nouveaux États indépendants; l'Afrique, l'Asie orientale et le Pacifique; le Proche-Orient et l'Afrique du Nord; l'Asie méridionale, le Bangladesh, l'Inde, le Pakistan et le Sri Lanka; l'Europe et la Turquie; la Chine, Hong-Kong et Taiwan; le Canada, les Antilles et l'Amérique latine, la construction aérienne et automobile et l'industrie de la défense dans le monde entier, les télécommunications, les technologies de l'information et l'industrie informatique dans le monde entier.

Il est l'interlocuteur central des entreprises et représente les différents services de l'administration américaine qui s'occupent de la promotion des exportations. Il intervient de manière non discriminatoire vis-à-vis des entreprises mais, en vertu de règles très claires, ne soutient que des projets conformes aux intérêts nationaux des États-Unis. Les produits fournis doivent, du point de vue de la valeur, provenir à 50 % au moins des États-Unis.

10.9.4.3. Participation de la CIA aux travaux du TPCC

Duncan Campbell a présenté aux membres de la commission certains documents, qui ne sont plus considérés secrets, prouvant une participation de la CIA aux travaux de l'Advocacy Center, notamment des procès-verbaux du Trade Promotion Coordinating Committee relatifs à des réunions du groupe de travail Indonésie tenues en juillet et août 1994[237]. Selon les documents en question, plusieurs collaborateurs de la CIA participent à ce groupe, qui doit concevoir une stratégie commerciale à l'égard de l'Indonésie. Ces collaborateurs sont nommément désignés dans les procès-verbaux.

De plus, il ressort des procès-verbaux que l'un des collaborateurs de la CIA estime que l'un des objectifs du groupe consiste à déterminer les concurrents principaux et à communiquer aux entreprises cette information de base[238].

---

[236] Page d'accueil de l'Advocacy Center, http://www.ita.doc.gov/td/advocacy/.

[237] TPCC Working Group Meeting, Agenda, 18.7.1994, TPCC Indonesia Advocacy-Finance Working Group, Distribution List, procès-verbal de la réunion du 17.8.1994, dossier de l'U.S. & Foreign Commercial Service du 25.8.1994.

[238] ibidem: “Bob Beamer suggested that any primary competitors known to the group for these projects should be included as background information”, Bob Beamer est l'un des représentants de la CIA .

10.9.4.4. Questions sans réponse

Le gouvernement américain n'a pas autorisé les entretiens que les membres de la commission souhaitaient avoir avec le Centre, lequel avait marqué son accord à cet effet. Deux questions qui suscitent des doutes n'ont donc pu être tirées au clair, ce que déplore votre rapporteur:

a) la commission dispose de documents (cf. chapitre 10, point 10.9.4.3.) qui établissent une participation de la CIA aux activités du TPCC,

b) dans les brochures d'information qu'il publie lui-même (citées précédemment), l'Advocacy Center indique qu'il mobilise les ressources de 19 "government agencies" des États-Unis. En d'autres endroits des brochures, il n'est fait état que de 18 agences. Pourquoi le nom de la dix-neuvième ne peut-il être rendu public?

Pour votre rapporteur, le refus d'autoriser les entretiens convenus avec l'Advocacy Center signifie qu'y ont lieu des activités dont le gouvernement américain ne souhaite pas parler.

10.10. Sécurité des réseaux informatiques

10.10.1. Importance du présent chapitre

Comme il a déjà été dit au chapitre 10, point 10.4, le piratage de réseaux informatiques ou le vols des données contenues dans les ordinateurs portables constitue actuellement la technique d'espionnage économique la plus efficace après l'utilisation d'espions. Les commentaires du présent chapitre n'ont pas directement trait à un système d'interception des communications internationales organisé à l'échelle mondiale. Compte tenu des objectifs de la commission, il n'est pas possible de renoncer dans le chapitre consacré à l'espionnage économique à un bref aperçu de l'un de ses instruments les plus efficaces. Une telle démarche est sans conteste utile pour juger de l'importance que revêt un système d'interception des communications internationales dans le contexte de l'espionnage économique.

10.10.2. Risque inhérent à l'utilisation de la technologie de l'information moderne dans les milieux économiques

Le traitement électronique des données a, depuis longtemps, envahi le monde économique. Des données de toutes sortes sont mémorisées de façon très compacte sur différents supports. Les données informatisées sont désormais l'un des principaux facteurs du savoir-faire des entreprises. S'il ouvre de nouvelles perspectives, le passage de la société industrielle à la société de l'information entraîne aussi des risques considérables sur le plan de la sécurité[239].

[239] Computerspionage, Dokumentation Nr. 44, Bundesministerium für Wirtschaft, juillet 1998.

10.10.2.1. Augmentation des risques

En résumé, les nouveaux risques apparaissant peuvent être décrits comme suit[240]:

De plus en plus d'entreprises sont en réseau et les informations toujours plus nombreuses qui sont compactées en un endroit peuvent facilement être recopiées par des pirates informatiques. Parallèlement, d'autres données sensibles sont décentralisées, ce qui rend difficile une gestion centrale de la sécurité. La mobilité des décideurs, qui emportent sur leurs ordinateurs portables des informations sensibles est à l'origine de risques supplémentaires. L'externalisation de services entraîne des transferts d'activités d'entretien, y compris dans le secteur des technologies de l'information, dont il conviendrait, du point de vue de la sécurité, de s'abstenir. L'importance relative attachée à la sécurité par la hiérarchie de l'entreprise entraîne, en combinaison avec les connaissances insuffisantes des décideurs en matière de sécurité, des décisions malheureuses.

10.10.2.2. Analyse détaillée des risques

Compression de l'information sur des supports compacts

De nos jours, les secrets des entreprises sont mémorisés de façon extrêmement concentrée sur des supports comprimés. Ainsi, il est possible de faire sortir d'une entreprise les plans complets d'une nouvelle unité sur un disque de la taille d'un paquet de cigarettes ou de l'extraire électroniquement, rapidement et sans trace, en piratant un réseau informatique.

Décentralisation des informations secrètes

À l'époque des gros ordinateurs, le contrôle de l'accès aux informations secrètes pouvait se concevoir simplement, dans la mesure où il ne fallait gérer qu'un seul ordinateur. Aujourd'hui, chaque utilisateur connecté au réseau dispose de capacités informatiques considérables à son poste de travail. S'il s'agit naturellement là pour l'utilisateur d'un avantage considérable, c'est aussi un désastre du point de vue de la sécurité.

Simplification du copiage des informations

À l'époque des plans dessinés à la main et des machines à écrire mécaniques, il était très difficile de copier de nombreux documents sans risquer d'être découvert. Aujourd'hui, à l'époque électronique, cela ne pose pas de problème. Les informations numériques peuvent être reproduites en quantité, facilement, rapidement et sans trace. Ainsi, l'acquisition du matériau souhaité ne nécessite souvent qu'une seule intervention. Le risque de découverte diminue donc de façon notable.

[240] *Roman Hummelt,* Wirtschaftsspionage auf dem Datenhighway, Hanser Verlag, Munich 1997.

Mobilité des décideurs

Les décideurs d'une entreprise emportent, souvent sans en être suffisamment conscients, sur leurs ordinateurs portables des informations d'importance stratégique pour l'entreprise. Dès lors qu'un disque dur peut être copié rapidement lors d'un "contrôle douanier" ou à l'occasion de la fouille d'une chambre d'hôtel, les possibilités des service de renseignement sont considérables. Autre risque: le vol, pur et simple, du carnet électronique. Par ailleurs, il est difficile, compte tenu de la décentralisation, d'intégrer dans une gestion centrale de la sécurité les contenus des disques durs des ordinateurs portables des décideurs d'une entreprise.

Externalisation de l'entretien

L'externalisation peut permettre à une entreprise de réduire ses coûts. Elle a cependant aussi pour effet, dans le domaine de la technologie de l'information et de l'entretien des installations téléphoniques, de donner à des techniciens extérieurs à l'entreprise accès à pratiquement toutes les informations. On ne saurait souligner suffisamment les risques qui en résultent.

Insuffisance de la gestion des réseaux

Parallèlement aux failles de sécurité du logiciel lui-même, que les pirates informatiques s'emploient en permanence à découvrir, le principal danger procède des administrateurs des réseaux, qui sont insuffisamment conscients des risques. Dans sa version de base, Windows NT est configuré de telle façon qu'il permet de découvrir quasiment toutes les informations sur le réseau, qui sont nécessaires pour réussir un piratage[241]. Si ces configurations et les mots de passe standard ne sont pas modifiés, l'accès au réseau est un jeu d'enfant. Une erreur répandue consiste également à consentir des dépenses importantes pour la sécurité de la cloison coupe-feu, sans protéger comme il se doit le réseau contre une attaque de l'intérieur[242].

10.10.3. Fréquence des attaques contre les réseaux

Le nombre des attaques contre les réseaux informatiques d'Internet augmente d'année en année[243]. Selon le Computer Emergency Response Team (CERT), organisation créée aux États-Unis en 1988 pour assurer la sécurité sur Internet, 132 incidents de sécurité ont été notifiés en 1989. En 1994, leur nombre était déjà passé à 2 241 et il atteignait, en 1996, 2 573. En l'occurrence, la zone d'ombre est extrêmement importante. Cette thèse est confirmée par une simulation à grande échelle réalisée sur ses propres ordinateurs par le ministère américain de la défense. On a tenté, de façon systématique, de pénétrer de l'extérieur dans 8 932 serveurs et unités centrales. Pour 7 860 systèmes, ces essais ont été fructueux, les essais n'étant découverts que 390 cas et notifiés que dans 19. On fait la distinction entre les attaques et les incidents de sécurité. Une attaque est une tentative isolée d'obtenir un accès sans autorisation à un système. Un incident de sécurité consiste en un certain nombre d'attaques conjointes. En extrapolant pour l'ensemble du réseau internet les résultats d'études portant sur une longue période, réalisées par le Pentagone et certaines universités américaines, il est

[241] *George Kurtz, Stuart McClure, Joel Scambray,* Hacking exposed, Osborne/McGraw-Hill (2000), 94.
[242] *Martin Kuppinger*, Internet- und Intranetsicherheit, Microsoft Press Deutschland (1998), 60.
[243] *Othmar Kyas,* Sicherheit im Internet, International Thomson Publishing (1998), 23.

possible d'estimer les incidents de sécurité et les attaques sur Internet à respectivement 20 000 et 2 millions par an.

10.10.4. Acteurs et méthodes

Les services de renseignement étrangers qui attaquent les système TI visent à parvenir, si posssible sans se faire remarquer, aux informations qui y sont contenues. En principe, il est possible de distinguer trois groupes d'acteurs et trois modes d'opération différents.

Acteurs internes avec droit d'accès général

Un espion introduit ou acheté qui arrive à occuper une fonction de gestionnaire de systèmes ou d'administrateur de la sécurité dans un centre informatique ne doit, pour exercer son activité d'espionnage et s'approprier quasiment l'ensemble du savoir-faire de son employeur, qu'utiliser les pouvoirs qui lui sont officiellement conférés. Il en va de même pour un ingénieur de développement dirigeant ayant un accès illimité à toutes les bases de données techniques de l'entreprise.

L'efficacité d'un tel espion est maximale. Il est toutefois exposé, en cas de suspicion, à un risque de découverte important, dès lors que les enquêtes se concentreront immédiatement sur le petit cercle de personnes ayant un accès général aux informations. De plus, il n'existe aucun moyen permettant de mettre un espion dans une situation lui garantissant un accès général; le hasard est le seul maître en l'occurrence.

Acteurs intérieurs avec droit d'accès localisé

Par rapport au pirate informatique qui agit de l'extérieur, un espion travaillant dans l'entreprise dispose d'un net avantage: il lui faut simplement vaincre l'obstacle de la sécurité du réseau et il n'est pas confronté en outre à une cloison coupe-feu. Depuis un poste de travail isolé, il est possible d'établir l'architecture du réseau, à condition de disposer des connaissances voulues, en utilisant les techniques des pirates informatiques extérieurs et les autres techniques accessibles aux personnes travaillant dans l'entreprise, et d'obtenir des informations considérables[244]. À cela s'ajoute que l'espion peut communiquer, sans éveiller le soupçon, avec d'autres membres de l'entreprise et que ce qu'il est convenu d'appeler le "social engineering" permet d'obtenir des mots de passe.

Si elle peut être grande, l'efficacité d'un tel espion ne saurait toutefois être aussi prévisible que dans le premier cas. Le risque de découverte est réduit, en particulier dans les réseaux où l'administrateur n'attache pas une importante suffisante à la possibilité d'une attaque interne. L'infiltration d'un espion ayant une formation technique lui permettant de pénétrer les réseaux informatiques est beaucoup plus simple (stagiaires, chercheurs extérieurs, etc.).

[244] *Anonymus*, Hacker's guide, Markt &Technik-Verlag (1999)

10.10.5. Piratage de l'extérieur

Il est connu et prouvé que des pirates informatiques ne cessent de pénétrer de l'extérieur dans les réseaux informatiques. Désormais, les services de renseignement forment également des spécialistes pour cela. L'efficacité d'une attaque par un pirate n'est ni prévisible ni planifiable; elle est fonction dans une grande mesure de la qualité de l'organisation de la défense et du fait, par exemple, que le réseau du département de recherche soit ou non matériellement connecté à Internet. Le risque pour l'espion professionnel est proche de zéro, même si l'attaque en tant que telle est découverte, car il ne doit pas être sur place pour agir.

10.11. Sous–estimation des risques

10.11.1. Conscience des risques dans les milieux économiques

La conscience du risque que représente l'espionnage économique n'est, jusqu'ici, pas très développée dans les milieux économiques. La preuve en est notamment donnée par le fait que souvent, les responsables de la sécurité font partie des cadres moyens et non de la direction de l'entreprise. La sécurité coûte cher, et les membres du comité de direction ne s'occupent la plupart du temps des questions de sécurité que lorsqu'il est trop tard.

Les grandes entreprises ont toutefois leurs propres services de sécurité ainsi que des spécialistes dans le domaine des TI. Par contre, les petites et moyennes entreprises ne disposent que très rarement d'experts en sécurité, et la plupart du temps, elles sont déjà bien contentes lorsque l'équipement informatique fonctionne tout simplement. Il n'empêche que de telles entreprises peuvent également être la cible de l'espionnage économique, dès lors qu'elles sont parfois très innovantes. De plus, les moyennes entreprises sous-traitantes sont, compte tenu de leur intégration dans le processus de production, de bonnes bases de départ pour des attaques sur les grandes entreprises.

10.11.2. Conscience du risque dans les milieux scientifiques

En règle générale, les chercheurs ne s'intéressent qu'à leur propre domaine spécialisé. Aussi sont-ils souvent une proie facile pour les services de renseignement. Votre rapporteur a appris, non sans un certain étonnement, que des instituts dont les activités s'orientent nettement sur la recherche appliquée, communiquent en clair par le courrier électronique et le réseau scientifique. C'est là de la folie pure et simple.

10.11.3. Conscience du risque dans les institutions européennes

10.11.3.1. Banque centrale européenne

Les informations concernant l'élaboration des décisions de la Banque centrale européenne pourraient revêtir une grande importance pour les services de renseignement. Que les marchés pourraient manifester un net intérêt en la matière, voilà qui se comprendrait naturellement. Au cours d'une réunion à huis clos, la commission a également entendu des représentants de la Banque centrale européenne au sujet des mesures de sécurité prises pour protéger les informations. Votre rapporteur a ainsi acquis le sentiment que la conscience du risque existait et que toutes les mesures de sécurité possibles étaient prises. Il dispose cependant d'informations[245] selon lesquelles la conscience du risque n'est pas aussi développée dans de nombreuses banques centrales nationales.

10.11.3.2. Conseil de l'Union européenne

Avant la désignation du Haut responsable pour la politique étrangère et de sécurité, le Conseil avait essentiellement axé ses efforts en matière de confidentialité sur la volonté de cacher au public et au Parlement européen le déroulement du processus de décision et l'attitude des gouvernements des États membres. Il n'aurait jamais pu se prémunir contre une opération de renseignement menée par des professionnels[246], dès lors, par exemple, que l'entretien des équipements techniques des cabines d'interprétation est confié à une firme israélienne. Le Conseil a désormais adopté des règles de sécurité[247] conformes aux normes de l'OTAN.

10.11.3.3. Parlement européen

N'ayant pas jusqu'ici eu à s'occuper de documents confidentiels, le Parlement européen n'a, en matière de protection du secret, ni une expérience ni une philosophie de sécurité. La nécessité ne s'en fera sentir qu'à partir du moment où le Parlement aura accès à des documents secrets. Dans tous les autres cas, il ne convient pas qu'une représentation démocratique, qui doit être aussi transparente que possible, se dote d'une politique générale du secret. Toutefois, il conviendrait, ne serait-ce que dans l'intérêt de la protection des informateurs et pétitionnaires, de pouvoir crypter, si besoin, le courrier électronique entre les différents bureaux de députés. Jusqu'ici, ce n'est pas possible.

---

[245] Communication privée, source protégée.
[246] Communication de membres du COREPER et de fonctionnairers du Conseil, sources protégées.
[247] Décision du Conseil du 19 mars 2001 adoptant le règlement de sécurité du Conseil, JO L 101 du 11.4.2001, pp. 1 et ss.

10.11.3.4. Commission européenne

À la Commission européenne, il existe des directions générales où, compte tenu de la nature des informations traitées, la confidentialité et la protection ne sont pas nécessaires. Bien au contraire, il convient qu'une transparence absolue soit la règle dans tous les domaines ayant trait avec la législation. Le Parlement européen devrait veiller à ce que, dans ces domaines, des règles de confidentialité hors de propos ne viennent inutilement masquer encore plus qu'aujourd'hui l'influence qu'exercent des firmes intéressées et d'autres tiers sur les propositions législatives.

Il existe toutefois également des secteurs de la Commission où des informations sensibles circulent. Il s'agit en particulier, outre Euratom, des relations extérieures, du commerce extérieur et de la concurrence. Sur la base des informations que la commission a obtenues des directions générales concernées à l'occasion d'une réunion à huis clos, et surtout d'autres informations en possession de votre rapporteur, il semble bien que l'on puisse véritablement douter de l'existence d'une conscience du risque que représente l'espionnage et d'une approche professionnelle de la sécurité au sein de la Commission européenne. Dans un rapport public, il ne convient pas, naturellement, de mettre en évidence les failles en matière de sécurité. Votre rapporteur estime néanmoins impérieux que le Parlement européen attache sans tarder toute l'attention voulue à cette question.

Aujourd'hui déjà, il est toutefois possible de constater que les systèmes de cryptage que la Commission utilise pour certaines parties de ses communications avec ses bureaux extérieurs sont surannés. Cela ne signifie pas que le niveau de sécurité soit mauvais. Les appareils utilisés ne sont toutefois plus produits et la moitié seulement des bureaux extérieurs disposent de possibilités de cryptage. Il est nécessaire de mettre en place d'urgence un nouveau système fonctionnant sur la base de courrier électronique crypté.

11. Le cryptage en tant qu'instrument d'autoprotection

11.1. Objectif et mode de fonctionnement du cryptage

11.1.1. Objectif du cryptage

Toute transmission d'informations porte en elle le risque que ladite information tombe aux mains de personnes non autorisées. Si l'on veut éviter que des tiers ne prennent connaissance des informations, il faut les placer dans l'impossibilité de lire ou d'écouter le message, c'est-à-dire crypter celui-ci. Dans le domaine militaire et diplomatique, les techniques de cryptage ont toujours été employées[248].

Au cours des vingt dernières années, l'importance du cryptage a grandi parce qu'un pourcentage sans cesse croissant des communications prennent le chemin de l'étranger, où le pays d'origine ne peut plus protéger le secret de la correspondance ou des communications. De plus, les possibilités techniques accrues dont dispose un État d'écouter ou d'intercepter légalement les communications débouchent sur un besoin accru de protection des citoyens préoccupés. Enfin, le désir accru des délinquants d'accéder illégalement aux informations, voire de les falsifier, a été à l'origine de mesures de protection (par exemple dans le secteur bancaire).

L'invention des communications électriques et électroniques (télégraphe, téléphone, radio, télécopieur, Internet) a notablement simplifié la transmission de l'information et l'a considérablement accélérée. Le hic est que cela ne s'est pas assorti d'une protection **technique** contre les écoutes/interceptions et que n'importe qui peut, à condition de disposer de l'appareillage nécessaire, intercepter une communication s'il a accès aux vecteurs. Effectuées de manière professionnelle, les interceptions ne laissent pas ou guère de traces. Le cryptage a donc pris une importance nouvelle. Le secteur bancaire a été le premier à utiliser systématiquement le cryptage pour protéger les communications auxquelles a donné lieu l'apparition de la monnaie électronique. L'internationalisation croissante de l'économie s'est également accompagnée, du moins dans une certaine mesure, du cryptage des communications. Les communications via Internet, non protégées, ont fait grandir le besoin éprouvé par les particuliers de mettre leurs communications à l'abri des écoutes.

La question se pose donc, dans le contexte du présent rapport, de savoir s'il existe des méthodes de cryptage des communications intéressantes du point de vue du coût, autorisées par la loi, suffisamment sûres et simples à appliquer pour se mettre à l'abri des écoutes.

11.1.2 Mode de fonctionnement du cryptage

Le principe du cryptage consiste à traiter un texte en clair de telle manière qu'il n'ait plus de sens ou qu'il ait un sens différent. Les initiés peuvent toutefois le décrypter. Lors du cryptage, une séquence pertinente de lettres est modifiée, de telle manière qu'une personne non initiée ne peut plus la comprendre.

[248] On en trouve la preuve jusque dans l'Antiquité, par exemple à Sparte au V^{e} siècle après Jésus-Christ.

Cela s'effectue suivant une méthode déterminée (algorithme de cryptage) reposant sur la permutation de lettres (transposition) et/ou le remplacement de lettres par d'autres (substitution). **La méthode de cryptage** (algorithme) n'est plus tenue secrète à l'heure actuelle. Au contraire, il a été procédé récemment à un appel d'offres public à l'échelle mondiale au sujet de la nouvelle norme mondiale de cryptage à utiliser dans le domaine économique. La même remarque s'applique à la réalisation d'un algorithme de cryptage déterminé pour tel ou tel appareil – par exemple un télécopieur crypté.

Ce qui est **secret**, c'est ce que l'on appelle la **clé**. Un exemple emprunté à un domaine apparenté permettra d'expliquer la situation. Le mode de fonctionnement des serrures est normalement connu de tous, ne serait-ce que parce qu'il est breveté. La protection d'une porte tient au fait que, pour un type déterminé de serrure, il peut y avoir de nombreuses clés différentes. Il en va de même du cryptage des informations: une méthode de cryptage **connue de tous** (algorithme) permet de tenir secrètes de nombreuses informations différentes grâce à des clés **tenues secrètes**.

Pour illustrer les notions évoquées ci-dessus, citons l'exemple du cryptage de César. Général romain, César cryptait les informations en remplaçant chaque lettre par celle venant trois lettres plus loin dans l'alphabet – A par D, B par E et ainsi de suite. Le codage du mot **ECHELON** donne alors le mot **HFKHORQ**. **L'algorithme** consiste ici **à déplacer les lettres** dans l'alphabet et la **clé** consiste à se décaler de **trois lettres dans l'alphabet**. Le cryptage et le décryptage s'effectuent de la même manière, à savoir en se décalant de trois lettres dans l'alphabet. Le procédé est donc symétrique. Aujourd'hui, un tel procédé n'assurerait pas une protection d'une seconde.

Une bonne méthode de cryptage peut être connue de tous tout en méritant quand même le qualificatif de sûre. Il faut pour cela que le nombre des clés possibles soit si grand qu'il devienne impossible de les essayer toutes dans un délai raisonnable, même en utilisant l'ordinateur. Toutefois, le nombre des clés (**brute force attack**) n'est pas en soi une garantie de sécurité dès lors que la méthode de cryptage débouche sur un texte offrant des éléments permettant le décryptage (par exemple fréquence de certaines lettres)[249]. Sous ces deux angles, le cryptage de César n'est pas une méthode sûre. En raison de la fréquence différente des lettres dans une langue, la simple substitution permet de forcer rapidement le procédé, d'autant qu'il n'y a que 25 possibilités de décalage, c'est-à-dire 25 clés, l'alphabet ne comptant que 26 lettres. À force d'essais, il est facile de trouver la bonne clé et de déchiffrer le texte.

Les caractéristiques d'un système sûr seront examinées ci-après.

[249] *Otto Leiberich*, Vom diplomatischen Code zur Falltürfunktion - Hundert Jahre Kryptographie in Deutschland, Spektrum der Wissenschaft, juin 1999, pp. 26 et ss.

11.2. Sécurité des systèmes de cryptage

11.2.1. Généralités

Demander qu'un système de cryptage soit sûr peut signifier deux choses. Premièrement, on attend peut-être qu'il soit absolument sûr, c'est-à-dire qu'il soit impossible de déchiffrer le message si l'on ne connaît pas la clé, cette impossibilité pouvant être prouvée mathématiquement. Deuxièmement, il peut suffire que le code ne puisse être forcé dans l'état actuel de la technique, la sécurité étant ainsi assurée temporairement, c'est-à-dire nettement plus longtemps que le laps de temps critique pendant lequel une information doit rester secrète.

11.2.2. Sécurité absolue: one-time pad

À l'heure actuelle, seul le one–time pad représente un procédé entièrement sûr. Il a été mis au point à la fin de la première guerre mondiale[250] et également appliqué ultérieurement aux téléscripteurs de crise entre Moscou et Washington. Il repose sur une clé constituée par une séquence tout à fait aléatoire de lettres, séquence qui n'est pas répétitive. L'expéditeur et le destinataire cryptent au moyen de ces séquences puis détruisent la clé après usage. Étant donné que la clé ne présente aucun ordre interne, il est impossible à un analyse de venir à bout du code. Cela peut être prouvé mathématiquement[251].

L'inconvénient du système tient au fait qu'il n'est pas facile de produire de grandes quantités de telles clés aléatoires[252] et qu'il est difficile et peu pratique de répartir les clés de manière sûre. La méthode n'est donc pas utilisée largement dans les transactions.

11.2.3. Sécurité relative en fonction de l'état de la technique

11.2.3.1 Utilisation de machines de cryptage et de décryptage

Dès avant l'invention du one–time pad, on avait mis au point des procédés de cryptage offrant un grand nombre de clés et produisant des textes cryptés présentant le moins possible de régularité, c'est-à-dire d'éléments permettant une analyse. Pour rendre ces méthodes praticables à bref délai, des machines de cryptage et de décryptage furent mises au point. La plus fameuse fut ENIGMA[253], employée par l'Allemagne durant la deuxième guerre mondiale. L'armée de spécialistes du décryptage en activité a Beltchley Park au Royaume–Uni parvint à venir à bout du cryptage d'ENIGMA grâce à des machines spéciales appelées "bombes". Comme ENIGMA, les "bombes" étaient des machines mécaniques.

---

250 Introduit par le major Joseph Mauborgne, chef du service cryptographique de l'armée américiane. Voir *Simon Singh*, Geheime Botschaften, Carl Hanser Verlag (1999), 151.

251 *Simon Singh*, Geheime Botschaften, Carl Hanser Verlag (1999), 151 et ss.

252 *Reinhard Wobst*, Abenteuer Kryptologie[2], *Adison-Wesley* (1998), 60.

253 Mise au point et brevetée en 1928 par *Arthur Scherbius*. Elle s'apparentait dans une certaine mesure à une machine à écrire car elle était munie d'un clavier qui permettait de transcrire le texte en clair. Un dispositif rotatif permettait le cryptage et le texte pouvait être décrypté avec la même machine grâce à des codes.

11.2.3.2. Utilisation de l'ordinateur

L'invention de l'ordinateur représenta une percée dans le domaine du cryptage car ses performances rendent possible l'emploi de systèmes de plus en plus complexes. Si cela ne change rien aux principes fondamentaux de cryptage, il y eut cependant des innovations. Pour commencer, le degré de complexité des systèmes de cryptage fut multiplié car le matériel n'était plus soumis aux contraintes de la mécanique. De plus, la vitesse de cryptage fut nettement accrue.

L'ordinateur traite l'information au moyen de nombres binaires. L'information est traduite sous forme de deux signaux, zéro et un. Un correspond à une tension électrique, zéro à l'interruption de la tension. Dans ce contexte, c'est la norme ASCII[254] qui s'est imposée: chaque lettre est représentée par une combinaison à 6 chiffres de 0 et de 1[255]. Un texte se présente donc sous la forme d'une multitude de 0 et de 1 et ce sont des chiffres et non des lettres qui sont cryptés.

Cela permet de recourir aux formules de transposition et de substitution. La substitution peut par exemple passer par l'insertion d'une clé prenant la forme d'une suite de chiffres. Suivant les règles de la mathématique binaire, la somme de chiffres identiques donne O (0+0=0 et 1+1=0). La somme de deux chiffres différents donne 1 (0+1=1). La nouvelle séquence cryptée résultant de l'insertion est donc une suite binaire qui peut être numérisée ou qui peut être rendue lisible en retirant la clé ajoutée.

L'ordinateur permet, grâce à des algorithmes de cryptage puissants, de produire des textes cryptés n'offrant pour ainsi dire aucune prise à l'analyse. Une tentative de décryptage ne peut plus être effectuée qu'en essayant toutes les clés possibles. Plus la clé est longue et plus la tentative est vouée à l'échec même si l'on utilise des ordinateurs très performants et si l'on y consacre le temps nécessaire. Il existe donc des méthodes praticables qui peuvent être considérées comme sûres à la lumière de l'état de la technique.

11.2.4. Normalisation et limites de la sécurité

La propagation de l'ordinateur au cours des années 70 a rendu plus nécessaire la normalisation des systèmes de cryptage, indispensable pour permettre aux entreprises de communiquer avec leurs partenaires en toute sécurité et moyennant un effort raisonnable. Les premières tentatives en ce sens eurent lieu aux États-Unis.

Un système de cryptage puissant peut aussi être utilisé à des fins malveillantes ou par un éventuel adversaire militaire. Il peut rendre difficile ou impossible l'espionnage électronique. C'est pourquoi la NSA demanda avec insistance qu'une norme de cryptage suffisamment sûre soit retenue pour l'économie. Elle conservait toutefois une possibilité de décryptage grâce à son équipement technique particulier. La longueur de la clé fut limitée à 56 bits. Cela réduit le

---

254 American Standard Code for Information Interchange.

255 A = 1000001, B= 1000010, C= 1000011, D= 1000100, E = 1000101, etc.

nombre des clés possibles à 100 000 000 000 000 000[256]. C'est le 23 novembre 1976 que le chiffre de Lucifer d'Horst Feistel fut officiellement adopté dans la **version à 56 bits** sous la dénomination de Data Encryption Standard (DES), qui fut durant un quart de siècle la norme de cryptage officielle américaine[257]. Elle fut adoptée en Europe et au Japon, notamment dans le secteur bancaire. L'algorithme de cette norme n'a jamais été percé, en dépit de ce qu'ont affirmé différents médias, mais il existe aujourd'hui des machines suffisamment puissantes pour essayer toutes les clés ("brute force attack"). La DES–Triple, dont la clé compte 112 bits, est toujours considérée comme sûre. Le successeur de la DES, à savoir l'AES (Advanced Encryption Standard) est une méthode européenne[258], conçue sous le nom Rijndael à Louvain, en Belgique. **Ce procédé est rapide et considéré comme sûr car il échappe à la contrainte de la longueur de la clé**. Cela s'explique par une modification de l'approche américaine.

La normalisation a représenté une simplification notable du cryptage pour les entreprises. Le problème de la distribution des clés subsiste cependant.

11.3. Problème de sécurité en matière de diffusion des clés

11.3.1. Cryptage asymétrique: procédé de la public–key

Aussi longtemps qu'un système fonctionne avec un clé permettant à la fois le cryptage et le décryptage (symétrie), il est difficile à utiliser avec de **nombreux** partenaires de communication. En effet, la clé doit être communiquée **préalablement** à chaque nouveau partenaire, et ce de telle manière qu'aucun tiers ne puisse en avoir connaissance. Dans la pratique, cela est très difficile dans le monde économique et possible seulement dans des cas isolés pour les particuliers.

Le codage asymétrique offre une solution: on n'utilise pas la même clé pour coder et pour décrypter. L'information est cryptée au moyen d'une clé qui peut être connue de tous et que l'on appelle la **clé publique**. Toutefois, le système fonctionne à sens unique: la clé publique ne permet pas le décryptage du texte. Toute personne qui souhaite obtenir une information cryptée peut transmettre sa clé publique à son partenaire par une voie peu sûre pour qu'il code l'information. Le décryptage de l'information reçue s'effectue au moyen d'une autre clé, la **clé privée**, qui est gardée secrète et n'est pas transmise[259]. La comparaison la plus éclairante pour comprendre ce système est celle du cadenas: n'importe qui peut le verrouiller et ainsi condamner un coffre, mais seule la personne qui possède la bonne clé peut l'ouvrir[260]. La clé publique et la clé privée ne sont pas dissociables, mais la clé publique ne permet pas de déterminer la clé privée.

Ron Rivest, Adi Shamir et Leonard Adleman ont mis au point un système de cryptage asymétrique appelé RSA. Le résultat de la multiplication de deux très gros nombres premiers est introduit à sens unique dans la clé publique. Cela permet de crypter le texte. Le décryptage

---

256 Ce nombre, sous forme binaire, compte 56 zéros et uns. Singh, Geheime Botschaften, Carl Hanser Verlag (1999), 303.

257 *Simon Singh*, Geheime Botschaften, Carl Hanser Verlag (1999), pp. 302 et ss.

258 Définie par deux cryptographes belges de l'Université catholique de Louvain , Joan Daemen et Vincent Rijmen.

259 L'idée du cryptage asymétrique (public–key) est due à Whitfield Diffie et Martin Hellmann.

260 *Simon Singh*, Geheime Botschaften, Carl Hanser Verlag (1999), p. 327.

n'est possible qu'à condition de connaître la valeur des deux nombres premiers utilisés. Il n'existe cependant aucune méthode mathématique permettant, à partir du résultat de la multiplication de deux nombres premiers, de calculer les nombres premiers d'origine. Pour l'heure, cela n'est possible qu'à force d'essais systématiques. En d'autres termes, le procédé est sûr compte tenu de l'état actuel des connaissances, dès lors que sont retenus des nombres premiers suffisamment élevés. Le seul risque réside dans le fait qu'un jour un mathématicien brillant pourrait trouver le moyen de décomposer les facteurs. Personne à ce jour n'est parvenu à le faire, en dépit d'efforts massifs[261]. Nombreux sont ceux qui affirment au contraire que le problème est impossible à résoudre, mais cela n'a pas encore été prouvé[262].

Par rapport aux procédés symétriques (par exemple DES) le cryptage au moyen d'une clé publique nécessite un délai de calcul beaucoup plus long ou le recours à des machines puissantes et rapides.

11.3.2. Cryptage par public–key pour les particuliers

Afin de rendre le système de public–key accessible à tous, Phil Zimmerman eut l'idée d'associer audit système, très exigeant du point de vue du calcul, un dispositif symétrique plus rapide. L'information est codée au moyen d'un système symétrique – le système IDEA développé à Zurich – cependant que la clé de cryptage symétrique est transmise simultanément grâce au système de public–key. Zimmerman créa un programme convivial – dénommé Pretty Good Privacy – qui créait les clés nécessaires en cliquant et opérait le cryptage. Le programme fut mis sur Internet, ce qui permettait à tout un chacun de le charger. PGP fut finalement racheté par l'entreprise américaine NAI mais toujours mis gratuitement à la disposition des particuliers[263]. Le code d'origine des premières versions a été publié, de sorte que l'on peut considérer qu'il n'y a pas de "porte de derrière". Le code d'origine de la nouvelle version PGP 7, qui se caractérise par un graphisme convivial, n'est malheureusement plus publié.

Il existe toutefois une autre application de la norme ouverte PGP, à savoir GnuPG. Celle-ci offre les mêmes méthodes de cryptage que PGP et est compatible avec PGP. Cependant, il s'agit d'un logiciel dont le code source est connu. Chacun peut l'utiliser et le communiquer. Le ministère fédéral de l'économie et de la technologie a soutenu la possibilité d'importer GnuPG sur Windows ainsi que le développement de l'aspect graphique mais les efforts en ce sens n'ont pas encore abouti. D'après les informations dont dispose le rapporteur, ils se poursuivent.

Il existe des normes concurrentes telles que S/MIME à laquelle adhèrent nombre de programmes de courrier électronique. Le rapporteur ne dispose d'aucune information concernant l'accès libre à ces solutions.

---

261 *Johannes Buchmann*, Faktorisierung großer Zahlen, Spektrum der Wissenschft 2 1999, pp. 6 et ss.
262 *Simon Singh*, Geheime Botschaften, Carl Hanser Verlag (1999), pp. 335 et ss.
263 Pour des informations sur le logiciel: voir www.pgpi.com.

11.3.3. Méthodes à venir

La cryptographie quantique pourrait ouvrir de nouvelles perspectives à la transmission sûre des clés: si la communication de la clé fait l'objet d'une interception, l'opération est détectée. Si l'on envoie des photons polarisés, la polarisation ne peut être constatée sans la modifier. Les intrus peuvent donc être détectés à coup sûr. Seule une clé qui n'a pas été interceptée est donc employée. Lors des essais, des transmissions sur 48 km de fibres optiques et sur 500 mètres dans l'atmosphère ont été couronnées de succès[264].

11.4 Sécurité des produits de cryptage

Dans le débat sur la sécurité réelle du cryptage, est sans cesse soulevé le problème que le produits américains comportent des "portes dérobées" (backdoors). Excel, par exemple, a fait la une des journaux: il a été avancé que dans la version européenne, la moitié de la clé apparaissait en clair dans le header. Microsoft a également attiré l'attention de la presse car un hacker a trouvé une clé NSA dans le programme, ce que Microsoft dément évidemment avec la dernière énergie. Étant donné que Microsoft n'a pas publié son code source, porter un jugement sur la question relève de la spéculation. En ce qui concerne les versions antérieures de PGP et de GnuPG, on peut exclure la présence d'une telle "backdoor" étant donné que le code source a été publié.

11.5 Cryptage et intérêts nationaux

11.5.1. Tentatives de limitation du cryptage

Certains pays interdisent l'utilisation de logiciels de cryptage ou d'appareils de cryptage et soumettent les dérogations à autorisation. Il s'agit notamment, mais pas seulement, de dictatures comme la Chine, l'Iran ou l'Irak. Les pays démocratiques aussi ont limité par la voie législative l'utilisation ou la vente de programmes ou de machines de cryptage. Les communications doivent être protégées des intrusions de particuliers mais l'État doit conserver la possibilité de procéder le cas échéant à des écoutes en toute légalité. La perte de supériorité technique des autorités doit être compensée par des interdictions juridiques. C'est ainsi que la France a frappé d'une interdiction générale l'utilisation de la cryptographie, la subordonnant à autorisation au cas par cas. En Allemagne, il y a eu débat voici quelques années sur la limitation du cryptage. Les États-Unis quant à eux ont limité la longueur des clés.

[264] Voir *Reinhard Wobst* , Abenteuer Kryptographie[2] , Adison-Wesley (1998), pp.234 et ss.

11.5.2. Importance d'un cryptage sûr pour le commerce électronique

Aujourd'hui, ces tentatives ont peut-être échoué définitivement. Au souci de l'État d'accéder au décryptage et, partant, aux textes en clair, s'opposent non seulement le droit au respect de la vie privée mais aussi des intérêts économiques concrets. En effet, le commerce et la banque électronique sont tributaires de communications sûres sur Internet. Si cela ne peut être garanti, ces formules sont vouées à l'échec car la confiance du client n'est plus assurée. Ce lien explique la mutation de la politique américano–française en matière de cryptage.

Il convient de faire observer ici que le commerce électronique a besoin de méthodes de cryptage sûres pour deux raisons: il faut non seulement crypter l'information, mais aussi pouvoir établir avec certitude l'identité du partenaire. La signature électronique peut passer par l'application inverse du procédé de public–key: la clé privée est utilisée pour crypter, la clé publique pour décrypter. Cette forme de cryptage confirme l'authenticité de la signature. Il est possible de se convaincre de l'identité d'une personne en utilisant la clé publique, mais la signature ne peut être imitée. PGP offre également cette fonction.

11.5.3. Problème des hommes d'affaires en déplacement

Dans de nombreux pays, l'utilisation de programmes de cryptage sur ordinateur portable est interdite aux hommes d'affaires en déplacement. Cela fait obstacle à toute protection des communications avec l'entreprise ou à la protection des données emportées contre les interceptions.

11.6. Problèmes pratiques du cryptage

S'agissant du problème des personnes qui peuvent avoir accès au cryptage, il semble opportun d'établir une distinction entre particuliers et entreprises.

Pour ce qui est des particuliers, il faut souligner que le cryptage de fax ou de conversations téléphoniques par cryptotéléphone ou fax crypté n'est pas faisable, notamment parce que les frais d'acquisition de ces dispositifs sont relativement élevés, mais aussi parce que leur utilisation suppose que le partenaire dispose du même équipement, ce qui n'est que très rarement le cas.

Le courrier électronique doit pouvoir être crypté par tout un chacun. À l'affirmation selon laquelle il n'y a pas de secret et, partant, rien à crypter, on peut répondre que les informations écrites ne sont normalement pas envoyées sur carte postale. Un courrier électronique non crypté n'est rien d'autre qu'une lettre sans enveloppe. Le cryptage du courrier électronique est sûr et ne pose pas de problème. Sur Internet, on trouve déjà des systèmes conviviaux tels que PGP/GnuPG, qui sont même mis gratuitement à la disposition des particuliers. Malheureusement, ils ne sont pas encore répandus. Il serait souhaitable que les pouvoirs publics montrent l'exemple et fassent du cryptage la règle afin de le démythifier.

En ce qui concerne les entreprises, il est indispensable que des informations sensibles ne soient transmises que grâce à des moyens de communication sûrs. Cela paraît évident, notamment pour les grandes entreprises, mais aussi pour les petites et les moyennes qui transmettent souvent par e-mail, sans cryptage, des informations internes et ce parce qu'elles ne sont pas suffisamment sensibilisées au problème. Il est à espérer que les associations professionnelles et les chambres économiques redoubleront leurs efforts d'information. Certes, le cryptage du courrier électronique n'est qu'un aspect de sécurité parmi de nombreux autres et il ne sert à rien lorsque l'information est accessible à des tiers avant d'avoir été cryptée. En d'autres termes, il faut sécuriser l'ensemble de l'environnement de travail afin d'assurer la sécurité des locaux et de contrôler l'accès physique aux bureaux et aux ordinateurs. Il faut aussi empêcher au moyen de fire-walls l'accès non autorisé à l'information via le réseau. L'interconnexion du réseau interne et d'Internet constitue un danger particulier. Dès lors que l'on se soucie de sécurité, il importe de n'utiliser que des systèmes dont le code source est public et a été vérifié. C'est la seule manière d'être certain de ce qu'il advient des données. Les entreprises ont donc beaucoup à faire dans le domaine de la sécurité. Sont déjà présentes sur le marché de nombreuses sociétés qui offrent des conseils et des services de sécurité à des prix raisonnables. L'offre suit la demande en hausse. Par ailleurs, il est à espérer que les associations professionnelles et les chambres économiques vont s'atteler à ce problème afin d'y sensibiliser les petites entreprises et de les aider à définir et à mettre en place un schéma global de protection.

12. Relations extérieures de l'UE et collecte de renseignements

12.1. Introduction

L'adoption du traité de Maastricht en 1991 a marqué la mise en place de la politique étrangère et de sécurité commune (PESC), nouvel instrument politique de l'Union européenne. Six ans plus tard, le traité d'Amsterdam étoffait la structure de la PESC et créait la possibilité d'initiatives de défense commune au sein de l'Union, sans préjudice des alliances existantes. Sur la base du traité d'Amsterdam et compte tenu de l'expérience du Kosovo, le Conseil européen de décembre 1999 (Helsinki) a lancé l'initiative de sécurité et de défense européenne. Cette initiative vise la création d'une force multinationale de 50 à 60 000 hommes pour la deuxième moitié de 2003. L'existence de cette force multinationale rendra inévitable la mise en place d'une capacité autonome en matière de renseignements. La simple intégration de celle de l'UEO serait insuffisante. Un renforcement de la coopération entre les services de renseignements des États membres allant bien au-delà de ce qui se fait actuellement, est inévitable.

Toutefois, le développement de la PESC n'est pas le seul élément qui devrait aboutir au renforcement de la coopération entre les services de renseignements de l'Union. Les progrès de l'intégration économique eux aussi rendent cette démarche nécessaire. Une politique économique commune suppose une perception commune de la réalité économique à l'extérieur de l'Union. Une position commune dans les négociations commerciales menées au sein de l'OMC ou avec les pays tiers suppose une protection commune. Des entreprises fortes en Europe supposent une protection commune contre l'espionnage économique venant de l'extérieur.

Enfin, il convient de souligner que le développement du deuxième pilier et des activités de l'Union dans le domaine de la justice et des affaires intérieures doit également déboucher sur un renforcement de la coopération entre les services de renseignements. La lutte contre le terrorisme, contre le trafic illicite d'armes, contre le trafic d'êtres humains et contre le blanchiment de l'argent ne peut se faire sans une coopération poussée entre les services de renseignements.

12.2. Possibilités de coopération au sein de l'UE

12.2.1. La coopération actuelle[265]

Il est de tradition depuis longtemps que les services de renseignements ne se fient qu'aux informations qu'ils recueillent eux–mêmes et qu'ils se méfient de leurs homologues. Il n'empêche que la coopération entre ces services se renforce progressivement. Des contacts fréquents ont lieu dans le cadre de l'OTAN, de l'UEO et de l'Union européenne. Si les services de renseignements de l'OTAN restent largement tributaires de l'apport considérable des États-Unis, la création du centre de satellites de l'UEO à Torrejon (Espagne) et celle d'une

[265] *Charles Grant,* Intimate relations. Can Britain play a leading role in European defence - and keep its special links to US intelligence? 4.2000, Centre for European Reform

section de renseignements au niveau du quartier général de l'UEO ont contribué à rendre l'Europe autonome dans ce domaine.

12.2.2. Avantages d'une politique commune dans le domaine du renseignement

Abstraction faite de l'évolution qui s'opère, il faut souligner les avantages que présenterait une politique commune en matière de renseignement.

12.2.2.1. Avantages pratiques

Premièrement, les informations secrètes ou non à collecter, à analyser et à évaluer sont trop nombreuses pour un seul organisme ou pour faire l'objet d'accords bilatéraux en Europe occidentale. Les activités des services de renseignements englobent la défense, les politiques économiques nationales et internationales, la lutte contre la criminalité et le trafic de la drogue. Même si elle n'existait qu'au niveau élémentaire, par exemple pour la collecte des renseignements (OSINT), la coopération donnerait des résultats d'une grande importance sous l'angle des politiques de l'Union.

12.2.2.2. Avantages financiers

Dans le passé récent, les budgets du renseignement ont fait l'objet de coupes sombres, démarche qui, dans certains cas, se poursuit. Simultanément, la demande d'informations a grandi. Il s'ensuit que la coopération serait non seulement possible, mais, à court terme, avantageuse. Elle serait intéressante notamment pour la mise en place et l'entretien d'infrastructures techniques ainsi que dans le domaine de l'évaluation des renseignements recueillis. La coopération accroîtrait l'efficacité de la collecte.

12.2.2.3. Avantages politiques

En principe, les renseignements recueillis sont utilisés pour permettre aux gouvernements de prendre des décisions mieux fondées. L'intégration politique et économique de l'Union suppose que les renseignements soient accessibles au niveau européen, ce qui nécessite plus d'une source.

12.2.3. Remarques finales

Ces avantages objectifs illustrent l'importance croissante de la coopération au sein de l'Union. Les États nations d'hier assuraient chacun de leur côté leur sécurité extérieure, l'ordre public intérieur, la prospérité nationale et l'identité culturelle. Aujourd'hui, l'Union européenne prend peu à peu un rôle qui est complémentaire à celui des États nations. Il est exclu que les services de renseignements soient le dernier ou le seul domaine à ne pas être touché par l'intégration européenne.

12.3. Coopération au–delà de l'Union

Depuis la deuxième guerre mondiale, la coopération dans le domaine de la collecte du renseignement s'est faite non au niveau européen mais au niveau transatlantique. Il est déjà apparu que des relations très étroites en matière de collecte de renseignements avaient été établies entre le Royaume–Uni et les États–Unis. Dans le domaine de la défense et dans le cadre de l'OTAN et au–delà de celui–ci, les États–Unis étaient et restent le partenaire dominant. La grande question est de savoir si le développement de la coopération européenne dans le domaine de la collecte de renseignements perturbera les relations avec les États–Unis ou entraînera le renforcement de ces relations. Comment les relations entre l'UE et les États–Unis évolueront–elles sous l'administration Bush? Comment les relations particulières entre les États-Unis et le Royaume-Uni se maintiendront-elles dans ce contexte?

D'aucuns estiment qu'il n'y a pas nécessairement contradiction entre les relations États-Unis Royaume-Uni et l'évolution de la PESC. D'autres sont d'avis que le problème de la collecte de renseignements peut être celui qui amènera le Royaume–Uni à déterminer si sa destinée est européenne ou transatlantique. Les liens étroits entre le Royaume–Uni et les États–Unis (et les autres parties à l'accord UKUSA) pourraient rendre plus difficile le partage de renseignements entre les autres États de l'Union, le Royaume–Uni se montrant peut être moins enclin à partager l'information à l'intérieur de l'Europe et les partenaires de l'UE se montrant moins confiants à l'égard du Royaume-Uni. De la même manière, si les États–Unis estiment que le Royaume–Uni a développé des liens spéciaux avec ses partenaires de l'UE, ils pourraient hésiter à partager l'information avec le Royaume-Uni. La coopération dans le domaine du renseignement peut donc constituer une pierre de touche des ambitions européennes du Royaume–Uni ainsi que de la capacité d'intégration de l'Union elle–même.

Dans les circonstances actuelles, il est peu vraisemblable que même des progrès rapides de la coopération entre les partenaires européens permettent, à court et même à long terme, de remplacer l'avantage technique des États–Unis. L'Union européenne ne sera pas en mesure de mettre en place un réseau évolué de satellites SIGINT et de stations au sol. L'Union européenne ne sera pas en mesure de mettre en place à court terme le réseau d'ordinateurs nécessaire pour faire le tri et analyser le matériel collecté. L'Union européenne ne sera pas disposée à mobiliser les ressources budgétaires nécessaires pour supplanter les efforts des États–Unis. Du point de vue technique et budgétaire, il est dans l'intérêt de l'Union de maintenir des relations étroites avec les États–Unis dans le domaine de la collecte du renseignement. Du point de vue politique aussi, il importe de maintenir et, au besoin, de renforcer les relations avec les États–Unis, notamment en ce qui concerne la lutte contre la criminalité organisée, le terrorisme, le trafic de drogue et d'armes et le blanchiment de l'argent. Des opérations communes sont nécessaires pour soutenir les efforts communs. Des actions communes en matière de maintien de la paix supposent une contribution accrue de l'Europe dans tous les domaines.

Cela dit, la sensibilisation de l'Europe doit s'accompagner d'une responsabilité accrue. L'Union européenne doit devenir un partenaire à part égale non seulement sur le plan économique, mais aussi dans le domaine de la défense et dans celui de la collecte du renseignement. Des capacités autonomes de l'Europe en matière de renseignements ne devraient pas être considérées comme affaiblissant les relations transatlantiques. Au contraire, elles devraient permettre de renforcer celles-ci en rétablissant l'équilibre et en faisant de

l'Union un partenaire plus performant. Parallèlement, l'Union doit s'employer de manière autonome à protéger son économie et ses entreprises contre des menaces telles que l'espionnage économique, la cybercriminalité et les attentats terroristes. Par ailleurs, la compréhension transatlantique est nécessaire dans le domaine de l'espionnage industriel. L'Union européenne et les États-Unis devraient convenir de normes concernant ce qui est autorisé et ce qui ne l'est pas dans ce domaine. Pour renforcer la coopération transatlantique, une initiative commune devrait être lancée au niveau de l'OMC: il s'agirait d'utiliser les mécanismes de cette organisation pour protéger un développement économique loyal dans le monde.

12.4. Remarques finales

Le développement d'une capacité commune de l'Union européenne en matière de renseignements doit être considéré comme nécessaire et inévitable, non sans maintenir l'indispensable protection de la vie privée des citoyens européens. La coopération avec les pays tiers, en particulier les États-Unis, doit être maintenue et si possible renforcée. Cela ne signifie pas nécessairement que les activités SIGINT de l'Europe doivent automatiquement être intégrées dans un système ECHELON indépendant pour l'Union européenne ou que l'Union doit devenir partenaire à part entière de l'accord UK/USA. Toutefois, l'exercice d'une responsabilité proprement européenne dans le domaine de la collecte du renseignement doit être sérieusement envisagé. Une capacité européenne intégrée dans ce domaine suppose un système de contrôle politique concernant ces activités. Des décisions devront être prises sur les moyens d'analyser les renseignements et de prendre les décisions politiques découlant de l'analyse. Faute d'un tel système de contrôle politique et donc d'une responsabilité politique, le processus de collecte d'informations porterait préjudice au processus d'intégration européenne.

13. Conclusions et recommandations

13.1. Conclusions

Existence d'un système mondial d'interception des communications privées et économiques (système ECHELON)

L'existence d'un système mondial d'écoutes des communications fonctionnant, avec la participation des États-Unis, des Royaume-Uni, du Canada, de l'Australie et de la Nouvelle-Zélande dans le cadre de l'accord UKUSA, ne fait plus de doute. Il peut être admis, eu égard aux indices disponibles et aux nombreuses déclarations concordantes émanant de milieux très divers, parmi lesquels des sources américaines, que pendant un certain temps du moins, le système - ou des parties de celui-ci – a porté le nom de code ECHELON. Ce qui compte, c'est qu'il est utilisé pour intercepter des communications privées et économiques mais non militaires.

L'analyse a montré que les possibilités techniques de ce système ne sont pas aussi grandes que ce que nombre de médias supposent. Néanmoins, il est inquiétant de constater que de nombreux responsables de la Communauté qui ont été entendus – notamment des membres de la Commission – ont déclaré n'avoir aucune connaissance de ce système.

Limites du système

Le système de surveillance repose principalement sur l'interception mondiale de communications par satellite. Or, dans les régions à forte densité de communications, seule une très modeste partie des communications s'effectue par satellite. Cela signifie que la majeure partie des communications ne peuvent être interceptées par des stations au sol mais uniquement par branchement sur câble ou par écoute radio. Les investigations ont montré que les pays UKUSA n'ont accès qu'à une partie très restreinte des communications par câble ou par radio et qu'en raison du personnel nécessaire, une partie plus limitée encore des communications peut être exploitée. Quelle que puisse être l'ampleur des moyens et capacités d'interception des communications disponibles, il est établi que le nombre extrêmement important des communications empêche, dans la pratique, un contrôle total et minutieux de l'ensemble des communications.

Existence d'autres systèmes d'écoute

Étant donné que l'écoute des communications est un moyen d'espionnage traditionnel des services de renseignements, un tel système pourrait être exploité par d'autres pays à condition qu'ils disposent des moyens financiers et des conditions géographiques nécessaires. Possédant des territoires outre mer, la France serait le seul État membre de l'UE, en mesure, géographiquement et techniquement, d'exploiter à elle seule un système d'écoute mondial. Il ressort de nombreux indices que la Russie exploite également un tel système.

Compatibilité avec le droit de l'UE

S'agissant de la compatibilité d'un tel système avec le droit de l'UE, il y a lieu de souligner que si ledit système n'est utilisé qu'à des fins de renseignements, il n'y a aucune contradiction avec le droit de l'UE dans la mesure où les activités qui relèvent de la sécurité de l'État ne sont pas couvertes par le traité CE. Elles ne relèvent que du titre V du traité UE (PESC), qui ne

contient encore aucune disposition en la matière, de sorte qu'une base fait défaut. Si le système est utilisé de manière abusive pour espionner la concurrence, il y a manquement à l'obligation de loyauté et atteinte à l'idée d'un marché commun où la concurrence est libre. Si un État membre participe à une telle démarche, il viole le droit de l'Union.

Lors de sa réunion du 30 mars 2000, le Conseil a clairement déclaré qu'il ne saurait accepter la création ou l'existence d'un système d'interception qui ne respecte pas les règles de droit des États membres et qui viole les principes fondamentaux visant à préserver la dignité humaine.

Compatibilité avec le droit fondamental au respect de la vie privée (article 8 de la convention des droits de l'homme)

Toute écoute de communication constitue une atteinte grave à la vie privée de la personne. L'article 8 de la convention des droits de l'homme, qui protège la vie privée, n'autorise des atteintes à celle–ci que pour préserver la sécurité nationale, à condition que les dispositions du droit national les prévoient et soient accessibles à tous, et qu'elles définissent les circonstances et conditions dans lesquelles les pouvoirs publics peuvent y recourir. Ces atteintes doivent être proportionnées et il doit donc y avoir mise en balance des intérêts en jeu, en sorte qu'il ne suffit pas qu'elles soient simplement opportunes ou souhaitables.

Un système de renseignements qui intercepterait, sans distinction et en permanence, les communications constituerait une violation du principe de proportionnalité et serait, partant, contraire à la CEDH. De la même manière, il y aurait violation de la convention si les dispositions en vertu desquelles la surveillance est opérée étaient dépourvues de fondement juridique, si celui–ci n'était pas accessible à tous ou s'il était formulé de telle manière que l'individu ne puisse percevoir ses conséquences. Étant donné que les dispositions sur la base desquelles les services de renseignements américains opèrent à l'étranger sont en grande partie secrètes, le respect du principe de proportionnalité est à tout le moins sujet à caution. Il n'en reste pas moins qu'il y a violation des principes d'accès au droit et de prévisibilité de ses effets énoncés dans la CEDH. Même si les États-Unis ne sont pas partie à la convention, les États membres doivent respecter celle-ci. Ils ne peuvent se soustraire aux obligations qu'elle leur impose en autorisant les services de renseignements d'autres pays soumis à des dispositions moins rigoureuses à opérer sur leur territoire. Autrement, le principe de l'égalité et ses deux composantes – accès et prévisibilité – serait privé de ses effets et la jurisprudence de la Cour des droits de l'homme serait vidée de sa substance.

La conformité aux droits fondamentaux d'une activité légale d'un service de renseignements suppose en outre que des dispositifs de contrôle suffisants soient prévus afin de parer aux risques inhérents à l'action secrète d'une partie de l'appareil administratif. Considérant que la Cour des droits de l'homme a souligné l'importance d'un système de contrôle efficace dans le domaine des activités de renseignements, il apparaît préoccupant que certains États membres ne disposent pas d'organes de contrôle parlementaires des services secrets.

Les citoyens de l'UE sont–ils suffisamment protégés des services de renseignements?

Étant donné que la protection des citoyens de l'UE dépend des situations juridiques qui existent dans les États membres, lesquelles sont très différentes, et dans certains cas caractérisées par l'absence d'organes de contrôle parlementaires, on ne peut guère parler de

protection suffisante. Même la où des organes de contrôle existent, la tentation est forte de s'intéresser davantage aux activités des services de renseignements intérieurs qu'aux activités extérieures étant donné que normalement les citoyens du pays ne sont concernés que dans le premier cas.

En cas de coopération entre services de renseignements dans le cadre de la PESC et autorités policières dans le cadre de la CJAI, les institutions sont invitées à mettre en place des dispositions de protection suffisantes pour les citoyens européens.

Espionnage économique

Il relève des missions des services de renseignements à l'étranger de s'intéresser aux données économiques tels que développement de branches, évolution des marchés des matières premières, respect d'embargos, respect des dispositions relatives à l'approvisionnement en biens à usage mixte, etc.. C'est la raison pour laquelle les entreprises exerçant des activités dans ces domaines sont généralement surveillées. Les services de renseignement des États-Unis ne se contentent toutefois pas de s'occuper de problèmes économiques généraux. Au motif de lutter contre les tentatives de corruption, ils interceptent également les communications des entreprises, et ce précisément dans le contexte de la passation des marchés. Une telle interception circonstanciée ne va cependant pas sans faire naître le risque de voir les informations détenues être utilisées aux fins non pas de la lutte contre la corruption mais bien de l'espionnage de concurrence, même si les États-Unis et le Royaume-Uni affirment qu'ils n'agissent pas ainsi. Dans ce contexte, il convient de faire observer que le rôle de l'Advocacy Center du ministère américain du commerce n'est toujours pas entièrement clair et qu'une rencontre convenue avec lui, qui aurait servi à clarifier les choses, a été décommandée par lui. Il y a également lieu de rappeler qu'en 1997 a été adoptée, dans le cadre de l'OCDE, une convention relative à la lutte contre la corruption des agents publics qui érige, à l'échelle internationale, les faits de corruption en infractions pénales. Ainsi, la corruption dans des cas d'espèce ne saurait-elle davantage justifier l'interception des communications.

En tout état de cause, il faut dire clairement qu'il n'est pas possible de tolérer une situation dans laquelle des services de renseignement sont utilisés pour l'espionnage de concurrence, espionnant des entreprises étrangères pour procurer des avantages concurrentiels aux entreprises nationales. Il n'existe toutefois aucun cas dans lequel il est prouvé que le système d'interception mondial faisant l'objet du présent rapport est utilisé à cette fin, contrairement à ce qui est souvent avancé.

En fait, les données sensibles se trouvent principalement à l'intérieur des entreprises de sorte que l'espionnage de concurrence consiste principalement à tenter d'obtenir des informations par le truchement de leurs collaborateurs ou de personnes infiltrées et de plus en plus souvent en pénétrant dans les réseaux informatiques. Ce n'est que lorsque les données sensibles sont acheminées vers l'extérieur par câble ou par radio (satellite) qu'un système de surveillance des communications peut être utilisé pour espionner. Trois cas se présentent:

- entreprises travaillant dans trois zones horaires, de sorte que les résultats intérimaires peuvent être envoyés d'Europe en Amérique puis en Asie;
- vidéoconférences d'entreprises multinationales se déroulant par satellite ou par câble;

- négociations de marchés importants sur place (construction d'usines, infrastructures de télécommunications, construction de systèmes de transport, etc.) lorsqu'il faut en référer à la maison mère à partir du site sur place.

Dans les petites et moyennes entreprises, la conscience du risque et du besoin de sécurité est malheureusement souvent insuffisante, et il est fréquent que le risque d'espionnage économique et d'interception des communications ne soit pas perçu. Dès lors qu'au sein des institutions européennes (à l'exception de la Banque centrale européenne et des directions générales "Relations extérieures" du Conseil et de la Commission), le sens de la sécurité n'est pas toujours très développé, il convient d'agir sans tarder.

Possibilités de protection

Les entreprises doivent protéger tout leur environnement de travail c'est–à–dire aussi les moyens de communication servant à transmettre des informations sensibles. Les systèmes de cryptage sûrs à prix abordable sont suffisamment nombreux sur le marché européen. Les particuliers doivent eux aussi être engagés à crypter leur courrier électronique, un courrier non crypté s'assimilant à une lettre sans enveloppe. Sur Internet, on trouve des systèmes conviviaux qui sont mis à la disposition des particuliers, parfois même gratuitement.

Coopération entre services de renseignements de l'UE

En décembre 1999, le Conseil européen a décidé, à Helsinki, de se doter d'une capacité militaire européenne plus efficace afin de pouvoir s'acquitter de l'ensemble des missions de Petersberg dans le contexte de la PESC. Pour atteindre cet objectif, l'Union européenne devra être en mesure, d'ici 2003, de déployer rapidement des forces militaires d'environ 50 000 à 60 000 personnes, qui seraient autonomes, disposant des capacités de commandement, de contrôle et de renseignement nécessaires. Les premiers pas dans la voie de la mise en place de telles capacités de renseignement ont déjà été franchis dans le cadre de l'UEO et du comité politique et de sécurité permanent.

Une coopération entre services de renseignements de l'UE apparaît indispensable car, d'une part, une politique commune de sécurité excluant les services secrets serait absurde et, d'autre part, cela comporterait de nombreux avantages d'ordre professionnel, financier et politique. Cela serait en outre conforme à l'idée d'un partenariat à égalité de droits avec les États–Unis et pourrait regrouper l'ensemble des États membres au sein d'un système mis sur pied dans le respect de la convention des droits de l'homme. Un contrôle par le Parlement européen devrait dans ce cas naturellement être assuré. Le Parlement européen est sur le point de transposer le règlement (CE) n° 1049/2001 relatif à l'accès du public aux documents du Parlement européen, du Conseil et de la Commission, et d'adapter son règlement en ce qui concerne l'accès aux documents sensibles.

13.2. Recommandations

Lutte contre l'espionnage économique

en ce qui concerne la conclusion et la modification des conventions relatives à la protection des citoyens et des entreprises

1. le Secrétaire général du Conseil de l'Europe est invité à soumettre au comité des ministres une proposition d'adaptation de la protection de la vie privé garantie à l'article 8 de la Convention relative aux droits de l'homme aux méthodes de communication et aux possibilités d'interception modernes, et ce dans un protocole additionnel ou dans le contexte de la réglementation relative à la protection des données, dans le cadre d'une révision de la Convention afférente, étant entendu que cela ne saurait déboucher sur un abaissement du niveau de protection assuré par la Cour des droits de l'homme ni sur une réduction de la souplesse nécessaire pour suivre l'évolution;

2. les États membres de l'Union européenne sont invités à mettre en place une plateforme européenne composée de représentants des organismes nationaux chargés de contrôler le bilan des États membres en matière de droits fondamentaux et de droits des citoyens afin de vérifier si les dispositions nationales régissant les services de renseignement sont compatibles avec la CEDH et avec la charte des droits fondamentaux de l'UE, plateforme qui serait également appelée à examiner les dispositions relatives à la garantie du secret de la correspondance et des communications. De plus, les États membres devraient se voir soumettre une recommandation relative à l'élaboration d'un code de conduite garantissant la protection de la vie privée, telle qu'elle est définie à l'article 7 de la Charte européenne des droits fondamentaux, à tous les citoyens européens sur le territoire des États membres et garantissant en outre que les activités des services de renseignements s'effectuent dans le respect des droits fondamentaux et, partant, des conditions énoncées au chapitre 8 du rapport, en particulier du point 8.3.4, en vertu de l'article 8 de la Convention relative aux droits de l'homme;

3. les États membres du Conseil de l'Europe sont invités à adopter un protocole additionnel permettant à l'Union d'adhérer à la Convention relative aux droits de l'homme ou d'envisager d'autres moyens d'éviter les conflits de jurisprudence entre la Cour européenne des droits de l'homme et la Cour de justice européenne;

4. les États membres sont invités à adopter, lors de la prochaine conférence intergouvernementale, la Charte des droits fondamentaux en tant qu'instrument contraignant et pouvant faire l'objet de recours afin d'améliorer le niveau de protection des droits fondamentaux, notamment en ce qui concerne la vie privée; les institutions européennes sont invitées, dans le cadre de leur sphère de compétence et d'action respective, à mettre en application les droits fondamentaux établis par la Charte;

5. l'Union européenne et les États-Unis sont invités à conclure une convention établissant que chacune des deux parties respecte à l'égard de l'autre les dispositions de protection de la vie privée des citoyens et de confidentialité des communications des entreprises applicables à ses propres citoyens et entreprises;

6. les États membres sont invités à conclure avec les pays tiers une convention visant à renforcer la protection de la vie privée des citoyens de l'Union, convention dans laquelle toutes les parties s'engagent à ce que, en cas d'interception pratiquée par l'une d'entre elles dans un autre pays signataire, la première informe ce dernier des actions envisagées;

7. le Secrétaire général des Nations unies est invité à charger l'organe compétent de l'Organisation de présenter des propositions visant à adapter l'article 17 de la Convention internationale relative aux droits civils et politiques, qui garantit la protection de la vie privée, aux innovations techniques;

8. les États-Unis sont invités à signer le protocole additionnel à la Convention internationale relative aux droits civils et politiques afin de rendre possibles, en cas de violation, les recours individuels devant la commission des droits de l'homme prévue par la Convention; invite les ONG américaines compétentes, notamment l'ACLU (American Civil Liberties Union) et l'EPIC (Electronic Privacy Information Center) à faire pression en ce sens sur le gouvernement américain;

9. le Conseil et les États membres sont instamment invités à se doter d'un système de contrôle démocratique de la capacité de renseignement européenne autonome ainsi que des autres activités de renseignement connexes au niveau européen, étant entendu que le Parlement européen doit jouer un rôle important dans ce système de contrôle;

en ce qui concerne l'action législative nationale en matière de protection des citoyens et des entreprises

10. les États membres sont instamment invités à vérifier la conformité aux droits fondamentaux, tels qu'ils sont définis dans la convention relative aux droits de l'homme et dans la jurisprudence de la Cour des droits de l'homme, de leur législation relative aux activités des services de renseignements et, au besoin, à lui apporter les adaptations nécessaires, ainsi qu'à reconnaître à tous les citoyens européens les mêmes garanties légales en ce qui concerne la protection de la vie privée et la confidentalité de la correspondance, étant entendu que si leurs lois relatives au pouvoir d'interception des services secrets établissent des discriminations, celles-ci doivent être supprimées;

11. les États membres sont invités à rechercher un niveau uniforme de protection vis-à-vis des activités des services de renseignements et à élaborer à cet effet un code de conduite qui se fonde sur le niveau de protection national le plus élevé, les citoyens concernés par les activités d'un service de renseignements étranger appartenant généralement à un autre pays, c'est-à-dire aussi à un autre État membre, un code de conduite analogue devant également être négocié avec les États-Unis;

12. les États membres sont invités à mettre en commun leurs moyens d'interception des communications afin de renforcer l'efficacité de la PESD dans les domaines du renseignement, de la lutte contre le terrorisme, la prolifération nucléaire ou le trafic international de stupéfiants, dans le respect des dispositions de protection de la vie privée des citoyens et de confidentialité des communications des entreprises, sous le contrôle du Parlement européen, du Conseil et de la Commission;

en ce qui concerne les mesures de lutte contre l'espionnage économique

13. les États membres sont invités à examiner si des dispositions du droit européen et international permettraient de lutter contre l'espionnage économique et la corruption visant à obtenir des marchés, notamment si une réglementation dans le cadre de l'OMC serait possible, qui tiendrait compte des distorsions de concurrence causées par de telles pratiques, par exemple en prévoyant la nullité de tels marchés; les États-Unis, le Canada, l'Australie et la Nouvelle-Zélande sont invités à se joindre à cette initiative;

14. les États membres sont invités à s'engager, sans réserve, à ne pas pratiquer, directement ou sous couvert, l'espionnage économique à l'encontre d'une puissance étrangère sur leur territoire et à ne pas autoriser, une puissance étrangère à le faire sur leur territoire, afin de respecter l'esprit et la lettre du traité CE;

15. les États membres et le gouvernement des États-Unis sont invités à nouer un dialogue franc sur la collecte de renseignements économiques;

16. les autorités du Royaume-Uni sont invitées à faire la lumière sur leur rôle dans l'alliance UKUSA étant donné que sont établies l'existence d'un système de type Échelon et son utilisation aux fins de collecte de renseignements économiques;

17. les États membres sont invités à s'assurer que leurs dispositifs de renseignements ne sont pas utilisés abusivement pour collecter des renseignements dans le cadre de la concurrence, au mépris de l'obligation de loyauté des États membres ainsi que de l'idée d'un marché unique fondé sur la libre concurrence;

en ce qui concerne l'application du droit et le contrôle de celle-ci

18. les États membrs sont invités à garantir un contrôle parlementaire et judiciaire approprié de leurs services secrets; les parlements nationaux qui ne disposeraient pas d'organe de contrôle parlementaire des services de renseignements sont invités à se doter d'un tel organe;

19. les organes de contrôle nationaux des services secrets sont invités à accorder une grande importance, dans l'exercice de leur pouvoir de contrôle, à la protection de la vie privée, que la surveillance concerne les ressortissants nationaux, les citoyens d'autres États membres de l'UE ou ceux de pays tiers;

20. les services de renseignements des États membres sont invités à ne se faire communiquer des informations par d'autres services de renseignements que lorsque celles-ci ont été obtenues dans des conditions prévues par le droit national, les États membres ne pouvant se soustraire aux obligations que leur impose la convention relative aux droits de l'homme en faisant intervenir des services de renseignements étrangers;

21. l'Allemagne et le Royaume-Uni sont invités à subordonner l'autorisation d'interception, sur leur territoire, de communications par les services de renseignements des États-Unis à la condition que cela se fasse dans le respect de la Convention relative aux droits de l'homme, c'est-à-dire conformément au principe de proportionnalité, que la base juridique soit accessible et que les effets soient prévisibles pour les personnes et qu'un contrôle

efficace soit prévu, étant donné qu'ils sont responsables de la conformité avec les droits de l'homme des activités de renseignements autorisées ou tolérées sur leur territoire;

en ce qui concerne la promotion de la protection des citoyens et des entreprises

22. la Commission et les États membres sont invités à informer les citoyens et les entreprises qu'il est possible que leurs communications internationales soient, dans certaines circonstances, interceptées, cette information devant être assortie d'une assistance pratique en matière de conception et de mise en œuvre de mesures de protection globales, incluant la sécurité des techniques d'information;

23. la Commission, le Conseil et les États membres sont invités à élaborer et à appliquer une politique efficace et active en matière de sécurité de la société de l'information, étant entendu qu'une attention particulière doit être accordée à la sensibilisation de tous les utilisateurs des systèmes de communication modernes en ce qui concerne la protection des informations confidentielles, et qu'un réseau européen coordonné d'organismes capables de fournir une assistance pratique en matière de conception et de mise en œuvre de stratégies de protection globale doit être mis en place ;

24. la Commission et les États membres sont invités à élaborer des mesures de promotion, de développement et de fabrication de matériels et de logiciels de cryptage européens et surtout à soutenir les projets visant à développer des logiciels de cryptage conviviaux dont le texte-source soit publié;

25. la Commission et les États membres sont invités à promouvoir des projets de logiciels dont le texte-source soit publié, étant donné qu'il s'agit là de la seule manière de garantir qu'ils ne comportent pas de "backdoors" ("open-source software"); la Commission est invitée à définir une norme du niveau de sécurité des logiciels destinés à l'échange de correspondances électroniques en plaçant les logiciels dont le code source n'est pas publié dans la catégorie la moins fiable;

26. les institutions européennes et les administrations publiques des États membres sont invitées à recourir systématiquement au cryptage du courrier électronique afin de faire de celui-ci la règle, à terme;

en ce qui concerne les mesures de renforcement de la sécurité dans les institutions

27. les institutions communautaires et les administrations publiques des États membres sont invitées à prévoir la formation de leur personnel et la familiarisation de celui-ci avec les nouvelles techniques de cryptage en organisant les stages et les cours de formation nécessaires;

28. la Commission est invitée à faire réaliser une analyse de sécurité destinée à préciser ce qui doit être protégé et à faire élaborer un schéma de protection;

29. la Commission est invitée à actualiser son système de cryptage, une modernisation s'imposant d'urgence, et l'autorité budgétaire (Conseil et Parlement) est invitée à prévoir les moyens financiers à cette fin;

30. la commission compétente est invitée à élaborer un rapport d'initiative sur la sécurité et la protection du secret dans les institutions européennes;

31. la Commission est invitée à assurer la protection des données dans le contexte du traitement interne et à renforcer la protection des documents non accessibles au public;

32. la Commission et les États membres sont invités à investir, dans le cadre du sixième programme cadre de recherche, dans les nouvelles techniques de cryptage et dans la recherche dans le domaine de la protection contre les tentatives de décryptage;

en ce qui concerne d'autres démarches

33. les entreprises sont invitées à coopérer davantage avec les services de contre-espionnage, à leur signaler les attaques extérieures relevant de l'espionnage économique, afin d'accroître leur efficacité;

34. la Commission est invitée à proposer la création, en coopération étroite avec les entreprises et les États membres, d'un réseau européen et coordonné de centres de conseil, notamment dans les États membres qui ne possèdent pas de tels organes**,** en matière de sécurité de l'information dans les entreprises qui, à côté de la sensibilisation, aurait pour mission d'apporter une aide pratique;

35. la Commission est invitée à attacher une attention particulière à la situation des pays candidats en matière de sécurité, étant entendu que ceux-ci devraient être aidés s'ils ne sont pas en mesure de se doter des moyens de protection nécessaires faute d'indépendance technologique;

36. le Parlement européen est invité à organiser un colloque non limité à l'Union sur la protection de la vie privée face à la surveillance des télécommunications afin de créer une plateforme permettant aux ONG d'Europe, des États-Unis et d'autres pays d'examiner les aspects transfrontaliers et internationaux et de coordonner les activités et démarches.

PARLEMENT EUROPÉEN

1999 *2004*

Document de séance

FINAL
A5-0264/2001
Par2

11 juillet 2001

RAPPORT

sur l'existence d'un système d'interception mondial des communications privées et économiques (système d'interception ECHELON)
(2001/2098(INI))

Partie 2: Avis minoritaires
Annexes

Commission temporaire sur le système d'interception ECHELON

Rapporteur: Gerhard Schmid

SOMMAIRE

Page

AVIS MINORITAIRE de Giuseppe Di Lello Finuoli, Pernille Frahm et Alain Krivine ……..... 4

AVIS MINORITAIRE de Patricia McKenna et Ilka Schröder 5

AVIS MINORITAIRE de Jean-Charles Marchiani 6

AVIS MINORITAIRE de Maurizio Turco 7

Annexe I: Liste des experts qui ont fourni des informations en commission 8

Annexe II: Sources documentaires 11

Annexe III: Interception des communications aux fins de poursuites pénales: définitions et commentaires 17

1. Remarques liminaires 17

2. Délimitation: interception des communications à des fins pénales/ à des fins de renseignement 17

3. Interception des communications à des fins pénales: travaux dans l'Union européenne 18

3.1 Généralités 18

3.2 Limitation de la compétence de l'UE aux réglementations techniques 18

3.3 Travaux et actes juridiques dans le domaine de l'interception des télécommunications 19

4. Travaux transfrontières dans le domaine de l'interception des télécommunications: définitions et commentaires 21

Annexe IV: 23

AVIS MINORITAIRE de Giuseppe Di Lello Finuoli, Pernille Frahm et Alain Krivine

Le rapport de la Commission affirme l'existence du système d'interception Echelon géré par différents Etats, parmi lesquels le Royaume Uni, Etat membre de l'Union européenne, avec la collaboration de l'Allemagne.

Un tel système d'interception indifférencié de communications, de données et documents viole le droit fondamental au respect de la vie privée garanti par les articles 8 de la Convention européenne des droits de l'Homme, et 6 du Traité de l'Union européenne.

Ce système viole donc de manière flagrante les libertés des citoyens européens, la logique du libre marché et la sécurité de l'Union ; quelle que soit notre appréciation ou opposition à ces logiques et à ces Traités, ces violations sont inacceptables.

Dans ses conclusions, le rapport aurait dû demander au Royaume Uni de se dissocier du système Echelon et à l'Allemagne de fermer la base d'écoutes située sur son territoire. On ne peut que regretter que l'Union européenne soit plus préoccupée par l'espionnage industriel que par les écoutes individuelles.

AVIS MINORITAIRE de Patricia McKenna et Ilka Schröder

En soulignant qu'ECHELON existe bel et bien, le présent rapport fait mouche. Mais il s'arrête au moment d'en tirer les conséquences politiques. Critiquer les interceptions pratiquées dans le cadre d'ECHELON, tout en participant à des projets visant à la création d'un service secret européen, voilà qui, de la part du Parlement européen, est bien hypocrite.

À l'échelle mondiale, il n'existe aucun mécanisme efficace de contrôle public des services secrets et de leurs pratiques antidémocratiques. Par nature, les services secrets ne peuvent être contrôlés. Ils doivent donc être supprimés. Le présent rapport sert à légitimer un service secret européen qui portera atteinte aux droits fondamentaux, tout comme le fait ECHELON.

La majorité du Parlement voit surtout une industrie dont l'espionnage industriel menacerait les profits. Or, la question vitale, c'est que les communications confidentielles sur longue distance sont devenues chose impossible. L'espionnage politique est une menace autrement plus grave que l'espionnage économique.

Outre qu'il minimise constamment les dangers qu'ECHELON présente à cet égard, le présent rapport passe sous silence les projets ENFOPOL d'interception dans l'Union européenne. Toute société est confrontée à ce choix fondamental: accepter ou refuser un contrôle permanent. En adoptant le présent rapport, le Parlement européen démontre qu'il ne se préoccupe pas de la sauvegarde des droits de l'homme et des libertés des citoyens.

AVIS MINORITAIRE de Jean-Charles Marchiani

C'est sans surprise que le groupe UEN a pris acte des résultats du vote sur le rapport de Monsieur Schmid, initialement censé concerner le système d'espionnage anglo-saxon Echelon.

La majorité de ce Parlement avait dès l'origine indiqué clairement ses intentions, en préférant cette commission ad hoc à l'instauration d'une véritable commission d'enquête. Elle n'avait alors plus rien à craindre de travaux où l'efficacité du rapporteur à faire systématiquement diversion n'était en rien menacée par un cartel de mécontents aux motivations trop disparates.

Notre message, lui, est limpide : les efforts de Monsieur Schmid n'ont pu occulter l'évidence de l'existence du système ECHELON, ni celle de l'implication active ou passive de plusieurs Etats membres.

Dès lors est constituée une sérieuse infraction aux principes des Traités qui aurait dû appeler à des sanctions ou, à tout le moins, à des mesures susceptibles d'éviter la subordination de la solidarité intra-européenne aux impératifs de la solidarité anglo-saxonne.

Le lourd rapport de Monsieur Schmid est riche d'informations, mais hors sujet.
Nous tenions donc à nous en démarquer, et à rejeter un fonctionnement qui permet à la fois à ce Parlement de prendre des sanctions « préventives » contre un gouvernement démocratiquement élu, et de s'en abstenir en pareille circonstance…

AVIS MINORITAIRE de Maurizio Turco

A. Alors même que l'on met en évidence l'existence probable d'un système anglo-américain "d'interceptions systématiques et généralisées à l'aide de moteurs de recherche", on omet de dire que cette capacité technologique est certainement utilisée par l'Allemagne et les Pays-Bas ainsi que, probablement, par la France. Il s'ensuit que – puisque les services secrets interceptent, au nom de la sécurité nationale et sans autorisation, des communications provenant de l'extérieur –certains États membres interceptent les communications d'institutions, de citoyens et d'entreprises d'autres États membres.

B. S'il favorise la protection de la vie privée, le renforcement du chiffrage suppose, par ailleurs, le renforcement des moyens de déchiffrage techniques et légaux, et cela en raison du lien indissoluble entre développement de systèmes cryptographiques, développement de systèmes de déchiffrage et développement de techniques d'interception.

C. Les solutions sont donc recherchées à l'échelon politique:

– contrôle juridictionnel et parlementaire des activités d'interception et surveillance des services de police, de sécurité et d'espionnage;
– empêcher la multiplication des autorités de contrôle qui appliquent des normes disparates en matière de protection des données, en l'absence d'un véritable contrôle démocratique et juridictionnel;
– arrêter des règles – dans le sens de la norme la plus élevée et sur la base de la jurisprudence de la CJCE – en matière de protection de la vie privée des citoyens européens contre les intrusions préventives des autorités publiques et éliminer les discriminations qui existent, dans l'Union, entre citoyens des États membres.

Annexe I: Liste des experts qui ont fourni des informations en commission

1. Membres de parlements nationaux

M. Arthur PAECHT, Assemblée nationale française
M. Armand De DECKER, président du Sénat belge
M^{me} Anne-Marie LIZIN, Sénat belge
M. Hans VAN HEVELE, secrétariat du Sénat belge
M. Guilherme SILVA, Parlement portugais
M. Ludwig STIEGLER, Bundestag, Allemagne
M. Dieter ANTONI, Parlement autrichien
M. Desmond O´MALLEY, Parlement irlandais

2. Représentants du secteur des services secrets

M. Ernst UHRLAU, coordinateur des services secrets à la Chancellerie fédérale d'Allemagne
M. Harald WOLL, Office du Bade-Wurtemberg pour la protection de la constitution, Allemagne

3. Experts en matière de télécommunications, de sécurité des réseaux et de sécurité informatique

M. José Manuel MENDES ESTEVES SERRA VERA, directeur technique, Banco Espirito Santo, Portugal
M. Clive FEATHER, directeur du développement "Logiciel", Demon Internet Ltd, Royaume-Uni
M. Jacques VINCENT-CARREFOUR, ancien chef de la division "Sécurité des réseaux", France Télécom
M. Bruno PELLERO, consultant spécialisé en matière d'écoute des télécommunications, Italie
MM. Erhard MÖLLER, Lutz BERNSTEIN et Bernd SCHINKEN, École technique supérieure, Aix-la-Chapelle, Allemagne

4. Auteurs et journalistes spécialistes d'ECHELON

M. Duncan CAMPBELL, Royaume-Uni
M. Bo ELKJAER, Danemark
M. Kenan SEEBERG, Danemark
M. James BAMFORD, Washington DC
M. Nicky HAGER, Nouvelle-Zélande

5. Experts en matière de cryptage

M. Reinhard WOBST, Unix Software, Allemagne
M. Bernd ROELLGEN, Ciphers GmbH, Allemagne
M. Peter BAHR, Ciphers GmbH, Allemagne
M. Johan KEMPENAERS, KBC Bank, Belgique

M. Leo VERHOEVEN, KBC Bank, Belgique
M. Bart PRENEEL, professeur de cryptologie, Université catholique de Louvain, Belgique
M. Danny de TEMMERMAN, Commission européenne
M. Desmond PERKINS, Commission européenne

6. Experts en matière d'espionnage économique et questions connexes

M. Sorbas VON COESTER, directeur de Salamandre (bureau de consultants), France
M. Christian HARBULOT, École de guerre économique, France
M. Thierry LA FRAGETTE, Circé, France
M. Ralf NEMEYER, Articon-Integralis, Allemagne

7. Droits de l'homme et protection de la vie privée

M. Dimitri YERNAULT, Université libre de Bruxelles
M. Simon DAVIES, Privacy International, Royaume-Uni
M. Jérôme THOREL, Privacy International, France
M. Yaman AKDENIZ, Cyber Rights and Cyber Liberties, Leeds, Royaume-Uni
MM. David NATAF et Alexandre COSTE, Millet-Sala-Nataf (bureau d'avocats), Paris
M. Rüdiger DOSSOW, Conseil de l'Europe, Strasbourg

8. Représentants d'institutions européennes

Commission européenne
Commissaire Christopher PATTEN (relations extérieures)
Commissaire António VITORINO (justice et affaires intérieures)
Commissaire Erki LIKKANEN (entreprises et société de l'information)
M. Lodewijk BRIET, direction générale des relations extérieures
M. Jacques DE BAENST, chef du protocole et de la sécurité
M^{me} Françoise DE BAIL, direction générale du commerce
M^{me} Susan BINNS, direction générale du marché intérieur

Conseil de l'Union européenne
M. Brian CROWE, directeur général des relations extérieures
M. Roland GENSON, représentation permanente du Luxembourg, justice et affaires intérieures
M. Hervé MASUREL, représentant de la présidence française en exercice
M. Gunnar LUND, ambassadeur, représentant de la présidence suédoise en exercice

Banque centrale européenne
MM. Christoph BOERSCH, Wolfgang SCHUSTER et Dominique DUBOIS, Banque centrale européenne

9. Interlocuteurs rencontrés lors de déplacements

Déplacement du président et du rapporteur à Paris, les 18 et 19 janvier 2001
M. Jean-Claude MALLET, secrétaire général, SGDN
M. Bertrand DUMONT, général de corps aérien, secrétaire général adjoint, SGDN

M[me] Claude-France ARNOULD, directeur des affaires internationales et stratégiques, SGDN
M. Henri SERRES, directeur chargé de la sécurité des systèmes d'information, SGDN
M. Stéphane VERCLYTTE, conseiller pour les affaires juridiques et européennes, SGDN
M. Philippe DULUC, conseiller pour les affaires scientifiques et techniques, SGDN
M. Gérard ARAUD, directeur des affaires stratégiques, ministère des affaires étrangères
M. Olivier MOREAU, directeur de la sécurité, ministère des affaires étrangères
M. Eric PERRAUDAU, conseiller, ministère de la défense
M. Jean-Pierre MILLET, avocat

Déplacement du président et du rapporteur à Londres, 24-26 janvier 2001
M. Tom KING, Chairman of the Intelligence & Security Committee, House of Commons
M. Alistair CORBETT, Head of the Secretariat of the ISC, House of Commons
M. Donald ANDERSON, Chairman of the Foreign Affairs Committee, House of Commons
M. Bruce GEORGE, Chairman of the Defence Committee, House of Commons
M. Jack STRAW, Secretary of State at the Home Office
M. Michael GILLESPIE, Security Service Coordinator
M. Charles GRANT, Director, Centre for European Reform
M. Casper BOWDEN, Director of FIPR

Déplacement du bureau de la commission, des coordinateurs et du rapporteur à Washington D.C., 6-12 mai 2001
H.E. Günter BURGHARDT, chef de la délégation de la Commission à Washington D.C.
M. James WOOLSEY, former Director CIA
M. Jeffrey RICHELSON, Director, National Security Archive, George Washington University
M. Marc ROTENBERG, Electronic Information Privacy Centre
M. Wayne MADSEN, Electronic Information Privacy Centre
M. David SOBEL, Electronic Information Privacy Centre
M. Barry STEINHARDT, Associate Director, American Civil Liberties Union
M. Porter J. GOSS, chairman House Permanent Select Committee on Intelligence
M[me] Nancy PELOSI, vice-chair House Permanent Select Committee on Intelligence
M. Robert DAVIS, Deputy Counsel for the office of Intelligence Policy Review, US Department of Justice

ANNEXE II: Sources documentaires

SOURCES CITÉES

Advocacy Center, Homepage, http://www.ita.doc.gov/td/advocacy/

Andrew, Christopher, The growth of the Australian Intelligence Community and the Anglo-American Connection, 223-224 in *E. Hayden, H. Peake and S. Halpern* eds, In the Name of Inteligence. Essays in honor of *Washington Pforzheimer* (Washington NIBC Press 1995), 95-109

Andrew, Christopher, The making of the Anglo-American SIGINT Alliance, in: *Hayden B. Peake, Halpern, Samuel*. (Eds.): In the Name of Intelligence. Essays in Honor of Walter Pforzheimer, NIBC Press (1995), 95 -109

Andronov, Major *A.*, Zarubezhnoye voyennoye obozreniye, Nr.12, 1993, 37-43

Anonymus, Hacker's guide, Markt &Technik-Verlag (1999)

Bamford, James, Body of Secrets. Anatomy of the Ultra-Secret National Security Agency. From the Cold War through the Dawn of a new Century, Doubleday Books (2001)

Bamford, James, The Puzzle Palace. Inside the National Security Agency, America's most secret intelligence organization, Penguin Books (1983)

Benett, Gordon, Conflict Studies and Research Center, The Federal Agency of Government Communications and Information, August 2000, http://www.csrc.ac.uk/pdfs/c105.pdf

Berliner Zeitung, Abgehört, 22.1.1996

Bode, Britta, Heinacher, Peter, Sicherheit muß künftig zur Chefsache erklärt werdenn Handelsblatt, 29.8.1996

Brady, Martin, Direktor der DSD, Brief vom 16.3.1999 an Ross Coulthart, Sunday Program Channel 9; http://sunday.ninemsn.com/01_cover_stories/transcript_335.asp; http://sunday.ninemsn.com/01_cover_stories/article_335.asp

Bronskill, Jim, Canada a key snooper in huge spy network, Ottawa Citizen, 24.10.2000, http://www.ottawacitizen.com/national/990522/2630510.html

Buchmann, Johannes, Faktorisierung großer Zahlen, Spektrum der Wissenschaft 2, 1999

Bundesministerium für Wirtschaft und Technologie der Bundesrepublik Deutschland, Computerspionage, Dokumentation Nr. 44, Juli 1998

Bundesministerium für Wirtschaft und Technologie der Bundesrepublik Deutschland, Informationen für geheimschutzbetreute Unternehmen (1997)

Bundesverfassungsgericht der Bundesrepublik Deutschland, BVerfG-Urteil, 1 BvR 2226/94 vom 14.7.1999 (zu Art. 10 GG, Gesetz zu Artikel 10 Grundgesetz)

Campbell, Duncan, Der Stand der Dinge der Fernmeldeaufklärung (COMINT) in der automatisierten Verarbeitung zu nachrichtendienstlichen Zwecken von überwachten mehrsprachigen Breitbandmietleitungssystemen und den öffentlichen Leitungsnetzen und die Anwendbarkeit auf die Zielbestimmung und -auswahl von COMINT einschließlich der Spracherkennung, Band 2/5, in: STOA (Ed), die Entwicklung der Überwachungsechnologie und die Risiken des Missbrauchs von Wirtschaftsinformationen (Oktober 1999), PE 168.184

Campbell, Duncan, Inside Echelon, Heise Online, 24.7.2000, http://www.heise.de/tp/deutsch/special/ech/6928/1.html

Comité permanent de contrôle des service de renseignement, Rapport d'énquête sur la manière dont les services belges de renseignement reagissent face à l'éventualité d'un système americain "echelon" d'interception des communications téléphoniques et fax en Belgique, http://www.droit.fundp.ac.be/textes/echelonfr.pdf

Commission on the Roles and Capabilities of the US Intelligence Community, Preparing for the 21st Century: An Appraisal of U.S. Intelligence, (1996) http://www.gpo.gov/int/report.html

Deutscher Bundestag, Sekretariat des PKGr, Die Parlamentarische Kontrolle der Nachrichtendienste in Deutschland (2000)

Domestic and External Security Secretariat, Department of the Prime Minister and Cabinet (Neuseeland), "Securing our Nation's Safety", Dezember 2000, http://www.dpmc.govt.nz/dess/securingoursafety/index.html

Dodel, Hans, Satellitenkommunikation, Hüthig Verlag (1999),

Elkjaer, Bo & Seeberg, Kenan, Echelon was my baby, Ekstra Bladet, 17.1.1999

Eser, Albin, Überhofer Michael, Huber Barbara (Eds), Korruptionsbekämpfung durch Strafrecht. Ein rechtsvergleichendes Gutachten zu den Bestechungsdelikten im Auftrag des Bayerischen Staatsministeriums der Justiz, edition iuscrim (1997)

Federation of American Scientists (FAS), Homepage, http://www.fas.org/

Fink, Manfred, Lauschziel Wirtschaft - Abhörgefahren und -techniken, Vorbeugung und Abwehr, Richard Boorberg Verlag, Stuttgart (1996)

Förster, Andreas, Maulwürfe in Nadelstreifen, Henschel Verlag (1997)

Frattini, Franco, Il ruolo dei servizi di informazione e sicurezza nel caso 'Echelon'. Relazione del comitato parlamentare per i servizi di informatione e sicurezza e per il segreto di stato. Approvata nella seduta del 29 novembre 2000, Trasmessa alle Presidenze il 19 dicembre 2000.

Freeh, Louis J, Statement for the Record, Hearing on Economic Espionage, House Judiciary Committee, Subcommittee on Crime, Washington DC, 9.5.1996

Freyer, Ulrich, Nachrichten-Übertragungstechnik, Hanser Verlag (2000)

Frowein, Jochen Abr., Peukert, Wolfgang, Europäische Menschenrechtskonvention[2], N. P. Engel Verlag (1996)

Frost, Mike in Fernsehinterview von NBC "60 Minutes" vom 27.2.2000, http://cryptome.org/echelon-60min.htm

Frost, Mike in Interview des australischen Senders Channel 9 vom 23.3.1999 http://www.geocities.com/CapitolHill/Senate/8789/sunday1.htm

Grant, Charles, Intimate relations. Can Britain play a leading role in European defence - and keep its special links to US intelligence? 4.2000, Centre for European Reform

Guisnel, Jean, L'espionnage n'est plus un secret, The Tocqueville Connection, 10.7.1998

Hager, Nicky, Secret Power. New Zealands´s Role in the international Spy Network, Craig Potton Publishing (1996)

Hager, Nicky, Exposing the global surveillance system, http://www.ncoic.com/echelon1.htm

Hoffmann, Wolfgang, Arbeitsgemeinschaft für Sicherheit der Wirtschaft e.V. (ASW), Aktuelle Anmerkungen zur Sicherheitslage der deutschen Wirtschaft, April 2001

Hummelt, Roman, Wirtschaftsspionage auf dem Datenhighway, Strategische Risiken und Spionageabwehr, Hanser Verlag (1997)

Intelligence and Security Committee (UK), Annual Report 1999-2000

Jacobs, Frnacis G, White, Robin C.A., The European Convention on Human Rights[2], Clarendon Press (1996)

Jauvert, Vincent, Espionnage - comment la France écoute le monde, Le Nouvel Observateur, 5.4.2001, Nr. 1900, S. 14 ff.

Kreye, Andrian, Aktenkrieger, Süddeutsche Zeitung, 29.3.2001

Kuppinger, Martin, Internet- und Intranetsicherheit, Microsoft Press Deutschland (1998), 60

Kurtz, George, McClure, Stuar, Scambray, Joel, Hacking exposed, Osborne/McGraw-Hill (2000)

Kyas, Othmar, Sicherheit im Internet, International Thomson Publishing (1998), 23

Landesamt für Verfassungsschutz Baden Württemberg, Wirtschaftsspionage, Die gewerbliche Wirtschaft im Visier fremder Nachrichtendienste, 10/1998

Legal Standards for the Intelligence Community in Conducting Electronic Surveillance, Bericht an den amerikanischen Congress Ende Februar 2000, http://www.fas.org/irp/nsa/standards.html

Leiberich, Otto, Vom diplomatischen Code zur Falltürfunktion - Hundert Jahre Kryptographie in Deutschland, Spektrum der Wissenschaft, Juni 1999

Lyle Robert, Radio Liberty/Radio fre Europe, 10.Februar 1999

National Security Councils (NSC), Homepage, http://www.whitehouse.gov/nsc

Madsen, Wayne in Fernsehinterview von NBC "60 Minutes" vom 27.2.2000, http://cryptome.org/echelon-60min.htm

Paecht, Arthur, Rapport d'information déposé en application de l'article 145 du règlement par la commission de la défense nationale et des forces armées, sur les systèmes de surveillance et d'interception électroniques pouvant mettre en cause la sécurité nationale, N° 2623 Assemblée nationale, enregistré à la Présidence de l'Assemblée nationale le 11 octobre 2000.

Paecht, Arthur, Rapport fait au nom de la Commission de la défense nationale et des forces armées sur la proposition de loi (N° 1497) de M. Paul Quilès et plusieurs de ses collègues tendant à la création d'une délégation parlementaire pour les affaires de renseignement, enregistré à la Présidence de l'assemblée nationale le 23. novembre 1999

Porter, Michael E., Competitive Strategy, Simon & Schuster (1998)

Richelson, Jeffrey T., Desperately seeking Signals, The Bulletin of the Atomic Scientists Vol. 56, No. 2/2000, pp. 47-51, http://www.bullatomsci.org/issues/2000/ma00/ma00richelson.html

Richelson, Jeffrey T., The U.S. Intelligence Community[4], Westview Press, 1999

Richelson, Jeffrey T., The National Security Agency Declassified, National Security Archive Electronic Breefing Book no. 24, George Washington University http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB23/index.html

Richelson, Jeffrey T., Ball, Desmond, The Ties That Bind, Boston Unwin Hyman (1985)

Richter, Nicolas, Klettern für die Konkurrenz, Süddeutsche Zeitung, 13.9.2000

Rötzer, Florian, Die NSA geht wegen Echelon an die Öffentlichkeit, Heise Online, 26.02.2000, http://www.heise.de/bin/tp/issue/download.cgi?artikelnr=6633&rub_ordner=special

Schmidt-Eenboom, Erich, Streng Geheim, Museumsstiftung Post und Telekommunikation Heidelberg, (1999)

Schütze, Arno, Wirtschaftsspionage: Was macht eigentlich die Konkurrenz? P.M. Magazin, Die Moderne Welt des Wissens (1998)

Shane Scott, Bowman Tom, America's Fortress of Spies, Baltimore Sun, 3.12.1995

Simon Singh, Geheime Botschaften, Carl Hanser Verlag (1999)

Smith, Bradley F., The Ultra-Magic Deals and the Most Secret Special Relationship 1940-1946, Presidio (1993)

Sorti, Francesco, Dossier esclusivo. Caso Echelon. Parla Luigi Ramponi. Anche I politici sapevano, Il Mondo, 17.4.1998

State Department Foreign Press Center Briefing, Subject: Intelligence Gathering and Democracies: The Issue of Economic and Industrial Espionage, Washington DC, 7.3.2000

Süddeutsche Zeitung, Haftstrafe wegen Spionage für Russland, 30.5.2000

TPCC, Broschüre über das Advocacy Center, Oktober 1996

Thaller, Georg Erwin, Satelliten im Erdorbit. Nachrichten, Fernsehen und Telefonate aus dem Weltall, Franzis Verlag, München (1999)

Weißes Haus, Archive, http://govinfo.library.unt.edu/npr/library/direct/orders/tradepromotion.html

Wessely, Wolfgang, Das Fernmeldgeheimnis - ein unbekannts Grundrecht?, ÖJZ 1999, 491 ff

Wirtschaftswoche "Antennen gedreht", Nr. 46/9, November 1999

Wirtschaftswoche "Nicht gerade zimperlich", Nr. 43/16, Oktober 1992

Wobst, Reinhard, Abenteuer Kryptologie, Adison-Wesley (1998)

Woolsey, James, Why America Spies on its Allies, The Wall Street Journal Europe, 22.3.2000

Woolsey, *James,* Remarks at the Foreign Press Center, Transskript, 7.3.2000, http://cryptome.org/echelon-cia.htm

Wright, Steve, An appraisal of technologies for political control, STOA interim study (1998) PE 166.499/INT.ST.

Yernault, Dimitri, "Echelon" et l'Europe. La protection de la vie privée face à l'espionnage des communications, Journal des tribunaux, Droit Européen 2000, S. 187 ff.

AUTRES SOURCES

Air Intelligence Agency (AIA), Homepage, http://www.aia.af.mil

America´s Military Community, Homepage, http://www.military.com

Barr, Bob, Barr moves to expose "project ECHELON", 9.11.1999, http://www.house.gov/barr/p_110999.html

Bundesnachrichtendienst, Die Nachrichtendienste der Bundesrepublik Deutschland, 2000, http://www.bundesnachrichtendienst.de/diensteb.htm

Bundesamt für Verfassungsschutz, Spionage gefährdet die Sicherheit und die Interessen unseres Landes, 2001, http://www.verfassungsschutz.de/arbeitsfelder/spion/page.html

Campbell, Duncan, Somebody´s listening, They´ve got it taped, 12.8.1988, New Statesman, http://jya.com/echelon-dc.htm

Central Intelligence Agency (CIA), Homepage http://www.odci.gov/index.html

Commander Submarine Force, U.S. Atlantic Fleet - Surveillance and Intelligence, http://www.sublant.navy.mil/roles.htm#survintel

Collingwood, John, Carnivore Diagnostic Tool, 16.8.2000, FBI-Press-Room http://www.fbi.gov/

Ecole de Guerre Economique, Homepage, http://www.ege.eslsca.fr/

Federal Bureau of Investigation (FBI), Homepage, http://www.fbi.gov

Frankfurter Allgemeine Zeitung, Niederländische Wirtschaftsspionage, 19.4.2000

Frankfurter Allgemeine Zeitung, Wirtschaftsspionage, 3.2.2001

Freeh, J. Louis, Wirtschaftsspionage, 28.2.1996, Ansprache vor dem Senat, http://www.fbi.gov

General Dynamics, Seawolf Class, http://www.gdeb.com/programs/seawolf/

Göbel, Jürgen, Kommunikationstechnik, Grundlagen und Anwendungen, Hüthig (1999)

Goss, J. Porter, Additional views of chairman Porter J. Goss, 2000, http://www.aclu.org/echelonwatch/goss.htm

Gralla, Preston, So funktioniert das Internet: ein virtueller Streifzug durch das Internet, Markt und Technik (1999)

Hager, Nicky, Wie ich Echelon erforscht habe, 11.04.2000, http://www.heise.de/tp/deutsch/special/ech/6728/1.html

Hayden, Michael, Statement for the record of House Permanent Select Committee on intelligence, 12.04.2000 http://www.nsa.gov/releases/DIR_HPSCI_12APR.HTML

Innenministerium Brandenburg, Abwehr von Wirtschaftsspionage, 1999

Kerr, M. Donald, Congressional Statement on Carnivore Diagnostic Tool, 6.9.2000, http://www.fbi.gov

Kerr, M. Donald, Congressional Statement on Internet and data Interception Capabilities Developed by FBI, 24.7.2000, http://www.fbi.gov

Mass, Christian, Satelliten Signale anzapfen und auswerten, Satellitenspionage für Einsteiger, Franzis Verlag, Funkschau Telekom, Poing 1998

Mathiesen, Thomas, On Globalisation of Control: Towards an Integrated Surveillance System in Europe, Statewatch Publication, 11.1999

Matschke, Klaus Dieter, Geheimdienste im Auftrag des Wettbewerbs, 5.9.1998, Seku Media Verlag Ingelheim

National Security Agency (NSA), Homepage, http://www.nsa.gov/

Preneel, Bart, Relative Security of Cryptographic, 18.11.1998, Presentation on Conference on Problems of Global Security

Schönleber, Claus, Verschlüsselungsverfahren für PC-Daten, Franzis Verlag, Poing 1995

Secretary of State for the Home Department, Interception of communication in the UK, Juni 1999

Sénat et Chambre des représentants de Belgique, 14.2.2000, Rapport d´activités 1999 du Comité permanent de contrôle des services de renseignements et de sécurité

Tenet, George, Statement by Director of Central Intelligence before the House Permanent Select Committee on Intelligence, 12.4.2000, http://sun00781.dn.net/irp/congress/2000_hr/tenet.html

The United States Navy, Homepage, http://www.navy.mil

The US Army Intelligence and Security Command (INSCOM), Homepage http://www.vulcan.belvoir.army.mil

The White House, Defending America's Cyberspace, National Plan for Information systems protection Version 1.0, 2000, The White House 2000

Ulfkotte, Udo, Marktplatz der Diebe, Wie die Wirtschaftsspionage deutsche Unternehmen ausplündert und ruiniert. Bertelsmann Verlag, München (1999)

V. Bülow, Andreas, Im Namen des Staates. CIA, BND und die kriminellen Machenschaften der Geheimdienste. Piper Verlag, München (1998)

Verfassungsschutz Brandenburg, Abwehr von Wirtschaftsspionage - eine Aufgabe des Verfassungsschutzes, 1999, http://www.brandenburg.de/land/mi/vschutz/wispion.htm

Wall, Stephen, Ständiger Vertreter des Vereinigten Königreichs bei der Europäischen Union, Brief an Kommissar Liikanen zu GCHQ, 21.3.2000

Wojahn, Jörg, Die globalen High-Tech-Schnüffler, 1.9.2000, Der Standard

Annexe III: Interception des communications aux fins de poursuites pénales: définitions et commentaires

1. Remarques liminaires

Dans le cadre des travaux de la commission, lors du débat sur l'admissibilité, les incidences et les dangers des systèmes d'interception mondiaux utilisés à des fins de renseignements, on a évoqué de façon répétée l'existence, dans l'Union européenne, de mesures et d'activités qui, certes, touchent à la question de l'interception des communications, mais qui relèvent du domaine de la coopération judiciaire en matière pénale.

Dans la partie principale du rapport, le rapporteur n'évoque pas ces mesures, car la question de la légitimité de l'interception des communications à des fins pénales ne doit pas être amalgamée avec la question de la légitimité de l'interception des communications à des fins de renseignement. Même si, dans les deux cas, il s'agit d'atteintes à la vie privée qui se justifient par des considérations de sécurité (au sens le plus large), ces deux types d'interceptions présentent cependant, par les méthodes et les objectifs, des différences telles que des réglementations qui pourraient sembler rationnelles et équilibrées pour un domaine ne le seraient pas forcément pour l'autre. L'opportunité et la proportionnalité des mesures pénales ne doivent donc pas être examinées dans le contexte de l'appréciation politique des opérations de renseignement.

Pour éviter tout malentendu, il convient ici de revenir sur certaines questions qui ont été soulevées et de définir certaines notions. Dans les paragraphes qui suivent, on commencera par indiquer les différences entre interception des communications aux fins de poursuites pénales et interception des communications aux fins de renseignement (2); ensuite, compte tenu des compétences de l'UE, on en présentera les actes juridiques qui touchent à l'interception des communications à des fins pénales (3); et, enfin, on explicitera encore d'autres notions qui ont été utilisées de façon répétée au sein de la commission à propos de travaux transfrontaliers dans le domaine de l'interception des communications (4).

2. Délimitation: interception des communications à des fins pénales / à des fins de renseignement

Si les services de renseignements étrangers interceptent les communications (comme dans le cas du système ECHELON), c'est non pour surveiller telle ou telle personne, mais pour surveiller de façon générale les activités déployées à l'étranger, et cela afin d'obtenir des informations importantes sous le rapport de la sécurité. Cette surveillance est exercée secrètement et n'est pas censée être un jour portée à la connaissance de l'opinion publique. En faisant valoir que seul le secret peut garantir la sécurité et que l'on n'a pas affaire à des sujets de droit au sens propre, on permet souvent à des services secrets d'opérer dans une zone grise du droit dans laquelle les réglementations sont peu claires et les contrôles lacunaires.

En revanche, l'interception des communications à des fins pénales vise à empêcher, en cas de soupçon, la personne de passer à l'acte, ou à sanctionner des délits. Ce sont les autorités nationales qui mettent en place les mesures d'interception. Si des mesures d'interception

doivent être mises en place à l'étranger, elles le sont par les autorités du pays en question, dans le cadre de l'entraide judiciaire. Comme ces interventions visent les sujets de droit proprement dits, il existe, depuis la chute des États policiers, des réglementations très précises et des mécanismes de contrôle efficaces qui assurent l'équilibre entre les intérêts en cause. Des mesures d'interception ne peuvent donc être mises en place, en cas de soupçon fondé, que dans des cas particuliers. Dans de nombreux États membres, il est nécessaire d'obtenir l'autorisation d'un juge. Même lorsqu'elle est secrète, l'interception vise à permettre l'utilisation des matériaux dans le cadre d'une procédure pénale publique, de sorte que l'autorité elle-même a intérêt à obtenir de façon légale les preuves recherchées.

3. Interception des communications à des fins pénales: travaux dans l'Union européenne

3.1 Généralités

En insérant dans le traité UE un titre "Politique étrangère et de sécurité commune", on a créé la possibilité d'une coopération entre services de renseignements à l'échelon européen. Mais il n'a pas encore été fait usage de cette possibilité. Dans la mesure où il en existe dans le cadre de l'Union européenne, réglementations et travaux dans le domaine de l'interception des communications portent exclusivement sur le volet pénal, c'est-à-dire sur la coopération dans les domaines de la justice et des affaires intérieures.

3.2 Limitation de la compétence de l'UE aux réglementations techniques

À l'heure actuelle, la question de la recevabilité de mesures d'interception relève exclusivement de la compétence nationale des États membres. En vertu du principe d'autorisation limitée, l'UE ne peut intervenir que là où des compétences lui sont reconnues conformément aux traités. Or, le titre VI du TUE "dispositions relatives à la coopération policière et judiciaire en matière pénale" ne prévoit pas une telle compétence. Dans le domaine de la coopération policière (article 30, paragraphe 1 du traité UE), une action en commun est exclusivement prévue pour des aspects opérationnels, c'est-à-dire ceux qui concernent la manière d'exécuter le travail de la police. En matière de coopération judiciaire, l'article 31 c) prévoit dans le cadre de l'action en commun "d'assurer la compatibilité des règles applicables dans les États membres", ce qui n'est recevable que si cela est "nécessaire à l'amélioration de cette coopération" et vise donc les dispositions spécifiques à la coopération. Et le "rapprochement des règles de droit pénal des États membres" visé à l'article 29, dernier tiret, se limite à la fixation de règles minimales relatives aux éléments constitutifs (article 31, lettre e). En résumé, on peut constater que la question des conditions de l'opportunité des mesures d'interception continue de relever du droit national. Le rapporteur n'a connaissance d'aucune tentative d'un État membre visant à toucher à cette compétence exclusivement nationale.

Les États membres ne peuvent donc coopérer sur la base des traités UE que sur la question de l'exécution des mesures d'interception recevables au titre du droit national, c'est-à-dire à un niveau inférieur. Dans les cas où les régimes juridiques nationaux autorisent une interception des télécommunications, l'État membre concerné doit pouvoir solliciter l'aide des autres États membres en vue de l'exécution technique de celle–ci. Quant à savoir si l'on considère comme positive ou négative la simplification technique recherchée qui apportera sans doute une plus

grande efficacité dans l'interception transfrontalière en vue des poursuites pénales précisément dans le domaine de la criminalité organisée, cela dépend sans doute beaucoup de la confiance dans son propre État de droit. Soulignons une fois encore que – quand bien même l'harmonisation technique simplifierait–elle l'interception transfrontalière et sachant qu'un abus ne peut pas toujours être évité –les conditions de la recevabilité d'une interception, qui sont régies par un droit purement national, ne sont pas affectées.

3.3 Travaux et actes juridiques dans le domaine de l'interception des télécommunications

Dans le domaine de l'interception des télécommunications, deux actes juridiques ont été jusqu'à présent arrêtés dans le cadre de l'UE: la résolution du Conseil du 17 janvier 1995 relative à l'interception légale des télécommunications, dont le contenu devait être étendu aux États tiers par le biais d'un mémorandum et pour lequel une proposition de "up–date" était prévue (les deux sont préparés dans "des documents ENFOPOL") et la Convention relative à l'entraide judiciaire en matière pénale.

Résolution du Conseil du 17 janvier 1995 relative à l'interception légale des télécommunications[266]

Cette résolution résulte, semble–t–il, de la coopération des experts au sein des séminaires ILET (voir plus bas); elle est conforme pour l'essentiel aux IUR (international user requirements).

Cette résolution a pour but de faire en sorte que tous les États membres créent les conditions techniques pour que les autorités puissent accéder aux données dans le cadre de leur autorisation nationale et, donc, exercer techniquement les pouvoirs que leur confère le droit national.

À cet effet, une annexe énumère des "spécifications" très détaillées des États membres dont le Conseil "prend acte", du fait qu'elles constituent "un condensé important des besoins des autorités compétentes pour la réalisation technique des mesures d'interception légale dans les systèmes modernes de télécommunications". Ces spécifications sont, par exemple, les possibilités de surveillance en temps réel ou la capacité de transmettre les communications interceptées à l'installation de surveillance par l'opérateur de réseaux. Dans la résolution, le Conseil se déclare favorable à ce que les spécifications soient prises en considération lors "de la définition et de l'exécution des mesures et demande aux États membres et aux ministres responsables de coopérer afin d'appliquer ces spécifications en ce qui concerne les opérateurs de réseaux et les fournisseurs de services".

Il convient de souligner ici que la forme de l'acte juridique choisie, la résolution, ne revêt aucun caractère contraignant et n'engage donc aucunement les États membres. L'émotion que cette résolution et les documents qui s'y rapportent ont suscitée est moins imputable au contenu qu'aux circonstances dans lesquelles ils ont été élaborés, en particulier au manque de transparence.

[266] JO C 329 du 4.11.1996.

Memorandum of Understanding

Dans le "Mémorandum of Understanding"[267] qui a suivi, certains États tiers ont été invités à transposer les spécifications techniques citées dans la résolution du Conseil du 17 janvier 1995. Il fallait en outre obtenir que les innovations techniques et les nouvelles spécifications qui en découlent soient communiquées au FBI ainsi qu'au secrétariat du Conseil, ce qui a été fait sachant que la production des techniques d'information est souvent aux mains d'entreprises multinationales, rendant ainsi indispensable la coopération avec les autorités de surveillance des États tiers dans lesquels sont implantés des sites de production importants.

Le mémorandum a été signé le 23 novembre 1995 par les États membres de l'UE et par la Norvège mais il ne l'a pas été par d'autres États tiers. Les États–Unis, l'Australie et le Canada ont seulement fait savoir par écrit qu'ils encourageront la transposition nationale dans leur pays[268].

Le texte, qui n'a malheureusement pas été publié à ce jour, a donné lieu à de nombreuses spéculations dans la presse.

Le projet de résolution du Conseil relative à l'interception légale des télécommunications dans le domaine des nouvelles technologies

Comme le rapporteur l'a déjà indiqué dans son rapport du 23 avril 1999[269], le projet de résolution du Conseil relative à l'interception légale des télécommunications dans le domaine des nouvelles technologies est un "up–date" de la résolution de 1995. La nouvelle résolution du Conseil précise que les "spécifications" de la résolution du Conseil de 1995, auxquelles viennent s'ajouter plusieurs spécifications nouvelles, sont également valables pour les nouvelles technologies de communication, par exemple par satellite et Internet, et que les termes techniques utilisés jusqu'à présent doivent être interprétés conformément à la nouvelle technologie (par exemple, identification d'un numéro de téléphone dans Internet). Le projet a été adopté par le Parlement européen[270], mais provisoirement gelé par le Conseil.

La Convention relative à l'entraide judiciaire en matière pénale[271]

Le second acte juridique est la Convention relative à l'entraide judiciaire en matière pénale. Dans ses articles 17 et suivants, elle traite de la question des conditions et de la nature de

---

[267] N° 10037/95 ENFOPOL, 112, non publié.
Voir la réponse écrite, du 16 décembre 1998, de M. Karl Schlögel, ministre autrichien de l'intérieur, à la question parlementaire du député Alexander Van der Bellen (4739/AB XX. GP).
http://www.parlament.gv.at/pd/pm/XX/AB/his/047/AB04739_.html

[268] C'est ce qu'a expressément déclaré M. Karl Schlögel, ministre autrichien de l'intérieur (cf. note précédente); répondant, le 14 mai 1997, lors de l'heure des questions, à la question orale H–0330/97 de Jonas Sjöstedt, Michiel Patijn, en sa qualité de président en exercice du Conseil, a indiqué, de façon quelque peu obscure, que les États-Unis, le Canada, l'Australie et la Norvège avaient également souscrit à "ces dispositions" (il se référait aux spécifications visées dans la résolution du Conseil du 17 janvier 1995).

[269] A4–0243/1999.

[270] Résolution législative portant avis du Parlement européen du 7 mai 1999, JO C 279 du 1.10.1999, p. 498.

[271] Acte du Conseil du 29 mai 2000 établissant – conformément à l'article 34 du traité sur l'Union européenne – la Convention relative à l'entraide judiciaire en matière pénale entre les États membres de l'Union européenne JO C 197 2000, p. 1, articles 17 et suivants.

l'entraide judiciaire en matière pénale qui doit être possible en ce qui concerne l'interception des télécommunications. Sans entrer dans les détails des réglementations, constatons seulement que la Convention ne porte aucunement atteinte aux droits de la cible, puisque l'État membre dans lequel celle–ci se trouve peut toujours refuser l'entraide judiciaire lorsque celle–ci n'est pas admissible en vertu du droit national.

4. Travaux transfrontières dans le domaine de l'interception des télécommunications: définitions et commentaires

En plus des multiples actes communautaires, les différents groupes de travail qui existent ou ont existé dans le domaine de la politique de sécurité ont souvent suscité la confusion. Dans les paragraphes qui suivent, on s'efforcera donc d'expliciter certaines des notions en question.

ILETS (International Law Enforcement Telecommunications Seminar)

Les séminaires ILET sont dus à une initiative du FBI. En 1993, le FBI a invité des autorités chargées de poursuites pénales et des services d'information d'États amis à assister, à Quantico, à une séance sur le thème de l'interception des télécommunications. Une grande partie des États de l'UE ainsi que l'Australie et le Canada y ont participé[272]. Depuis lors, des rencontres ont régulièrement lieu en vue d'examiner les impératifs d'une surveillance efficace des communications à l'échelon international.

Au cours d'une rencontre à Bonn, en 1994, les membres des ILETS se sont mis d'accord sur un document comportant des orientations politiques dans l'annexe duquel figure une liste de "International user requirements" (IUR 1.0 ou IUR 95). Celle–ci contenait des critères qui devaient être imposés aux différents opérateurs de télécommunications en vue de simplifier le processus d'interception. Ces IUR 1.0 servaient – fût–ce de manière informelle – de base à la résolution du Conseil du 17 janvier 1995 relative à l'interception légale des télécommunications. Par la suite, d'autres réunions d'experts sur le thème des IUR et leur éventuelle transposition et adaptation aux nouvelles télécommunications ont été organisées.

Groupe TREVI

Dans le cadre du groupe TREVI, les ministres de la justice et des affaires intérieures des États membres de la CE ont examiné certaines questions de sécurité intérieure avant l'entrée en vigueur du traité de Maastricht (qui a introduit les dispositions relatives à la coopération dans le domaine de la justice et des affaires intérieures). Le groupe TREVI ne fonctionne plus, étant donné que les sujets sont traités entre temps au sein des groupes de travail spécifiques du Conseil.

Dans le domaine à l'examen, mentionnons essentiellement deux groupes de travail: le groupe "Entraide judiciaire en matière pénale", qui a examiné la Convention relative à l'entraide judiciaire en matière pénale dans le cadre de la coopération "justice et affaires intérieures", et le groupe de travail "Coopération policière" qui se penche sur les questions de l'interception légale des télécommunications, y compris celle des nouveaux systèmes de communication

[272] Voir la réponse écrite de M. Schlögel, ministre autrichien de l'intérieur, à la question parlementaire du député Van der Bellen 4014/AB XX.GP). http://www.parlinkom.gv.at/pd/pm/XX/AB/texte/040/AB04014_.html.

(téléphones mobiles, Internet, e-Mail); ce groupe s'est également penché sur le rapprochement des normes des spécifications imposées par les autorités d'interception agréées aux exploitants de réseaux et aux prestataires de services.

"ENFOPOL"

Contrairement à ce que croient de nombreux auteurs, ENFOPOL n'est ni un groupe de travail ni une organisation, mais une abréviation qualifiant des documents de travail en matière de poursuites pénales et d'affaires policières, comme le groupe de travail "Coopération policière"[273]. Ces documents ne portent pas l'entête ENFOPOL, mais sont classés en fonction de celui–ci.

[273] Réponse écrite de M. Schlögels, ministre autrichien de l'intérieur à la question parlementaire du député Van der Bellen (4014/AB XX.GP) http://www.parlinkom.gv.at/pd/pm/XX/AB/texte/040/AB04014_.html.

Annexe IV

TABLEAU SYNOPTIQUE

DES SERVICES DE RENSEIGNEMENT ET DES ORGANES DE CONTRÔLE PARLEMENTAIRE

DES ÉTATS MEMBRES

ET DES ÉTATS UKUSA

Pays	Service de renseignement	Base juridique	Missions	Renseignement électromagnétique	Organe de contrôle	Ba
AUTRICHE	**Heeresnachrichtenamt (HnA)** **Abwehramt (AbwA)** service de renseignement militaire sous l'autorité du ministre de la défense	*§ 20 Abs 3 Militärbefugnisgesetz (MBG) BGBl I 86/2000*	collecte de renseignements militaires; protection contre les activités étrangères constituant des menaces pour la sécurité		sous-commission parlementaire: *Ständiger Unterausschuss des Landesverteidigungsausschusses zur Überprüfung von nachrichtendienstlichen Maßnahmen zur Sicherung der militärischen Landesverteidigung (14 membres; chaque parti représenté au Parlement doit être représenté au sein de la sous-commission).* *1 commissaire à la protection des droits.*	*A B ge* *§§ G 19*
AUTRICHE	**Sondereinheit für Observation (SEO)** service de renseignement civil sous l'autorité du ministre de l'intérieur	*§§ 6, 14, 15 Sicherheitspolizeigesetz (SPG, BGBl 566/1991 idgF)* *Sondereinheiten-Verordnung (BGBl II 207/1998)*	préservation de la sécurité publique; contre-espionnage sur le territoire national; protection des principes faisant l'objet d'une garantie de la Constitution; lutte contre les mouvements extrémistes, le terrorisme et la criminalité organisée		sous-commission parlementaire: *ständiger Unterausschuss des Ausschusses für innere Angelegenheiten zur Überprüfung von Maßnahmen zum Schutz der verfassungsmäßigen Einrichtungen und ihrer Handlungsfähigkeit (14 membres; chaque parti représenté au Parlement doit être représenté au sein de la sous-commission).* *1 commissaire à la protection des droits.*	

Pays	Service de renseignement	Base juridique	Missions	Renseigne-ment électro-magnétique	Organe de contrôle	Ba
BELGIQUE	**Service Général du Renseignement et de la Sécurité des Forces armées (S.G.R.)** service militaire de renseignement et de sécurité sous l'autorité du ministre de la défense nationale	*Loi du 30 novembre 1998 organique des services de renseignement et de sécurité*	collecte d'informations et de données dans les domaines militaire, politique, économique et technico-scientifique; protection de la sécurité des installations et du personnel militaires.		*Comité permanent de contrôle des services de renseignements et de sécurité (Comité permanent R),* composé de trois membres nommés par le Sénat, qui n'ont pas le droit d'exercer un mandat électif ou une autre activité de nature à compromettre leur indépendance. *Service d'enquêtes des services de renseignements* subordonné au Comité permanent R; ses membres sont désignés par le Comité R.	*Lo (V co de re*
BELGIQUE	**Sûreté de l'État (V.S.)** service civil de renseignement et de sécurité sous l'autorité du ministre de la justice	*Loi du 30 novembre 1998 organique des services de renseignement et de sécurité*	Sécurité intérieure et extérieure, contre-espionnage, observation des mouvements politiques extrémistes			

Pays	Service de renseignement	Base juridique	Missions	Renseigne-ment électro-magnétique	Organe de contrôle	Ba
DANEMARK	Forsvarets Efterretningstjeneste (FE(T)) "Service secret de la défense" sous l'autorité du ministère de la défense	*Lov om forsvarets formål, opgaver og organisation m.v.* *Lov 909 af 8/12/1993* ["loi-cadre", sauf mention du FE(T)] [FET et PET feront prochainement l'objet d'une nouvelle loi]	collecte et analyse, aux fins de la défense, d'informations secrètes sur la CEI et l'Europe centrale et orientale dans les domaines militaire, politique, économique et technico-scientifique; renseignement électro-magnétique; chiffre; effectif et budget: informations classées	oui	2 commissions de contrôle: *Kontroludvalget vedrørende Politiets og Forsvarets efterretningstjenester (Wamberg-udvalget) (composée de fonctionnaires et d'avocats)* membres désignés par le ministre de la justice	pa sp
DANEMARK	Politiets Efterretningstjeneste (PET) "Service secret de la police" sous l'autorité du ministère de la justice	aucune législation spécifique [FET et PET feront prochainement l'objet d'une nouvelle loi]	contre-espionnage, prévention des activités de nature à mettre en danger la sécurité du pays et lutte contre ces activités: espionnage, terrorisme, etc.; sécurité du gouvernement et de la famille royale effectif: 370 personnes environ (1998) budget: informations classées.		*Udvalget vedrørende efterretningstjenesterne* commission parlementaire (composée de 5 membres du Folketing)	*Lo et fo ef lo*

Pays	Service de renseignement	Base juridique	Missions	Renseigne-ment électro-magnétique	Organe de contrôle	Ba
FINLANDE	**Pääesikunnan tiedusteluosasto** "Section du renseignement militaire du personnel de défense de la Finlande" sous l'autorité du ministère de la défense	*Laki puolustusvoimista* N:o 402/1974 2§ "Loi relative aux forces de défense" (qui ne mentionne pas la section du renseignement)	surveillance du territoire et de l'espace aérien du pays en collaboration avec d'autres organes de surveillance en vue d'assurer l'intégrité territoriale du pays	oui	aucun organe spécifique de contrôle le ministère de la défense présente chaque année au médiateur parlementaire un rapport sur les interceptions	*P* *§3* "L po *La m 40* "L m co [s m m pa co in m co
FINLANDE	**Suojelupoliisi (SUPO)** "La police de sécurité finlandaise" sous l'autorité du ministère de l'intérieur	*Laki poliisin hallinnosta N:o 110/1992, 1§, 10§ 1. ja 2. momentti Asetus poliisin hallinnosta N:o 158/1996 8§* *Laki poliisin henkilörekistereistä N:o 509/1995 23§, 9§* "Loi et décret sur l'administration de la police" et "loi relative au traitement par la police des données à caractère personnel "	contre-espionnage; prévention des activités de nature à mettre en danger la sécurité intérieure du pays et les relations internationales; lutte contre le terrorisme; action préventive pour la sécurité		aucun organe spécifique de contrôle; la police est tenue de rendre compte de tous les cas d'interception au ministère de l'intérieur, qui présente un rapport annuel au médiateur parlementaire	
FINLANDE	**Tullin tiedusteluyksikkö** "Section de renseignement des douanes finlandaises" ministère des finances	*Tullilaki N:o 1466/1994* "Loi relative aux douanes"	collecte et analyse de données en vue de la prévention et de la découverte des infractions douanières et transmission de ces données aux services compétents pour suites à donner		aucun organe spécifique de contrôle l'administration des douanes est tenue de rendre compte de tous les cas d'interception à l'office national des douanes et au ministère de l'intérieur, qui présente un rapport annuel au médiateur parlementaire	

Pays	Service de renseignement	Base juridique	Missions	Renseigne-ment électro-magnétique	Organe de contrôle	Ba
FRANCE	**Direction générale de la sécurité extérieure (DGSE)** sous l'autorité du ministère de la défense	*décret n°82-306 du 2 avril 1982*	collecte de renseignements d'intérêt politique, militaire, économique et technico-scientifique recherche et exploite des renseignements intéressants la sécurité de la France; contre-espionnage (hors du territoire national) Effectif: 4100 personnes; budget: FRF 1,7 milliards	oui	aucun organe parlementaire spécifique de contrôle (projet en discussion; la commission de la défense de l'Assemblée nationale a proposé, à deux reprises, la création d'un comité de surveillance; n^{os} 1951 et 2270) Commission nationale de contrôle des interceptions de sécurité (exclusivement le contrôle des écoutes sur câbles) composée, entre autres, d'un député et d'un sénateur.	

Pays	Service de renseignement	Base juridique	Missions	Renseigne-ment électro-magnétique	Organe de contrôle	Ba
	Direction du renseignement militaire (DRM) ministère de la défense	*décret n°92-523 du 16 juin 1992*	Fournit les renseignements militaires nécessaires aux armées Effectif: 1700 personnes; budget: FRF 90 millions; sécurité militaire intérieure, soutien de l'armée			
FRANCE	**Direction de la surveillance du territoire (DST)** service de renseignement civil sous l'autorité du ministre de l'intérieur	*décret n°82-1100 du 22 décembre 1982*	contre-espionnage sur le sol français effectif: 1500 personnes; préservation de la sécurité publique, contre-espionnage sur le territoire national			

Pays	service de renseignement	Base juridique	Missions	Renseigne-ment électro-magnétique	Organe de contrôle	Ba
ALLEMAGNE	**Bundesnachrichten-dienst (BND)** sous l'autorité du chancelier fédéral	*Gesetz über den Bundesnachrichten-dienst (BNDG),* BGBl 1990 I 2954 idgF	collecte et exploitation d'informations sur les pays étrangers qui présentent un intérêt pour la sécurité et la politique extérieure	oui	*Parlamentarisches Kontrollgremium (PKGR*) organe de contrôle parlementaire des trois services secrets; composé de 9 membres du Bundestag *G 10-Kommission* indépendante; peut, mais ne doit pas nécessairement, être composée de députés; 4 membres nommés par le PKGR.	*G Ko di de (P 19 id* *§ G G (G Au 94 (Id re du po té*
ALLEMAGNE	**Bundesamt für Verfassungsschutz (BfV)** sous l'autorité du ministre de l'intérieur	*Gesetz über die Zusammenarbeit des Bundes und der Länder in Angele-genheiten des Ver-fassungsschutzes und über das Bundsamt für den Verfassungsschutz* (BVerfSchG, BGBl 1090 I 2954)	collecte et exploitation d'informations sur les activités mettant la sécurité en danger et sur les activités des services de renseignement hostiles sur le territoire national			
ALLEMAGNE	**Militärischer Abschirmdienst (MAD)** sous l'autorité du ministre de la défense	*Gesetz über den militärischen Ab-schirmdienst (MADG*) BGBl 1990 I 2954 idgF	assurer le fonctionnement efficace de l'armée fédérale ainsi que la sécurité des installations et du personnel militaires.			

Pays	Service de renseignement	Base juridique	Missions	Renseigne-ment électro-magnétique	Organe de contrôle	Ba
GRÈCE	Ethniki Ypiresia Pliroforion (EYP) "Service national de renseignement" sous l'autorité du KYSEA (Conseil national de la sécurité: Premier ministre + ministres des affaires étrangères et de la défense nationale)	*loi 1645/86 relative au Service national de renseignement (Ethniki Ypiresia Pliroforion)*	- collecte et traitement d'informations en rapport avec la sécurité nationale (sur la criminalité organisée et le terrorisme) et de renseignements militaires, économiques et politiques; transmission aux autorités compétentes - contre-espionnage, observation des activités des agents de renseignements étrangers agissant contre le pays		commission parlementaire spéciale pour la protection du secret des communications et de la vie privée. Pas de droit de contrôle particulier. Composition: 1 vice-président du Parlement, 1 député par groupe politique, 1 spécialiste des communications.	lo *A e* (s co
					Office pour la protection des données à caractère personnel	lo *P e d p* (P tr d p

Pays	Service de renseignement	Base juridique	Missions	Renseigne-ment électro-magnétique	Organe de contrôle	Ba
IRLANDE	**Garda Síochána** (police nationale) chargée des questions relevant de la sécurité nationale La police est responsable devant le ministre de la justice	pouvoir d'interception en vertu de l'*Interception of Postal Packets and Telecommunications Messages (Regulation) Act 1993*	interceptions autorisées dans l'intérêt de la sûreté de l'État		*le Joint Committee on Justice, Equality and Women's Rights* a compétence pour tout le champ des droits civils	
IRLANDE	Intelligence Staff		protection de la sécurité du pays (principalement à l'égard de l'IRA), sécurité des forces armées nationales, évolutions technologiques des armées étrangères		Pas d'autorité de contrôle spéciale.	

Pays	Service de renseignement	Base juridique	Missions	Renseigne-ment électro-magnétique	Organe de contrôle	Ba
ITALIE	**Servizio per le informazioni e la sicurezza militare (SISMI)** **Servizio informazione Operative Segrete (SIOS)** soumis au ministre de la défense, qui désigne le directeur du Service et les hauts fonctionnaires	*L. 24 ottobre 1977, n. 801, art. 4 Istituzione e ordinamento dei servizi per le informazioni e la sicurezza e disciplina del segreto di Stato*	tâches d'information et de sécurité pour la défense, au niveau militaire, de l'indépendance et de l'intégrité de l'État; contre-espionnage; collecte d'informations étrangères sur des thèmes politiques, militaires, économiques et technico-scientifiques		Commission parlementaire (4 députés +4 sénateurs) Le gouvernement soumet au Parlement un rapport semestriel sur la politique d'information et de sécurité.	L. 80 *Is or se in si de*
ITALIE	**Servizio per le informazioni e la sicurezza democratica (SISDE)** **Direzione investigazioni anti-mafia (DIA)** soumis au ministre de l'intérieur, qui désigne le directeur du Service et les hauts fonctionnaires	*L. 24 ottobre 1977, n. 801, art. 6 Istituzione e ordinamento dei servizi per le informazioni e la sicurezza e disciplina del segreto di Stato*	tâches d'information et de sécurité pour la défense de l'État démocratique et de ses institutions informations sur les activités mettant la sécurité en danger sur le territoire national; contre-espionnage, lutte contre le terrorisme et la criminalité organisée			

Pays	Service de renseignement	Base juridique	Missions	Renseigne-ment électro-magnétique	Organe de contrôle	Ba
LUXEMBOURG	**Service de renseignement** service national d'information et de sécurité sous l'autorité du ministre d'État (=président du gouvernement)	*Loi concernant la protection des secrets intéressant la sécurité extérieure de l'État* du 30 juillet 1960	assurer la protection des secrets visés à l'art. 120 octies du Code pénal* et rechercher les informations que requiert la sauvegarde de la sécurité extérieure du Grand-Duché de Luxembourg et des États avec lesquels il est uni par un accord régional en vue d'une défense commune * "infractions commises envers le Grand-Duché de Luxembourg."		pas de contrôle parlementaire (la surveillance de toutes les formes de communications aux fins de rechercher des infractions contre la sûreté de l'État requiert l'assentiment d'une commission composée du président de la Cour supérieure de Justice, du président du Comité du contentieux du Conseil d'État et du président de la Chambre des comptes)	(L 19 in d' de 2,

Pays	Service de renseignement	Base juridique	Missions	Renseigne-ment électro-magnétique	Organe de contrôle	Ba
PAYS-BAS	**Militaire Inlichtingendienst MID**, ou bien MIVD plus récemment sous l'autorité du ministère de la défense	*Wet op de inlichtingen- en veiligheidsdiensten Loi 635/87 du 3 décembre 1987, dernier amendement loi 194/1999 du 19 avril 1999.* [Actuellement en discussion une toute nouvelle loi]	service de renseignement militaire; collecte d'informations sur les armées étrangères	oui	*Tweede-Kamercommissie voor de Inlichtingen- en veiligheidsdiensten* "Commission auprès de la 2e Chambre des services de renseignements et de sécurité intérieure" Commission parlementaire (4 membres: présidents des 4 partis les plus grands)	*17 or Ka G* "R Cl An po d' Se
PAYS-BAS	**Binnenlandse Veiligheidsdienst** (**BVD** ou bien le AIVD plus récemment) sous l'autorité du ministère de l'intérieur		service de renseignement intérieur; lutte contre l'extrémisme de droite et de gauche; contre-espionnage			

Pays	Service de renseignement	Base juridique	Missions	Renseigne-ment électro-magnétique	Organe de contrôle	Ba
PORTUGAL	**Serviçio de Informaçoes Estratégicas de Defesa e Militares (SIEDM)** dépend du ministre de la défense	Loi 30/84 du 5 septembre 1984, modifiée par la loi 4/95 du 21 février 1995; loi 15/96 du 30 avril 1996; et loi 75–A/97 du 22 juillet 1997	service de renseignement pour l'étranger; service de renseignements stratégiques sur les questions politiques, militaires et économiques		*Conselho de Fiscalização dos Serviços de Informações (CFSI).* organe composé de trois citoyens élus par l'Assemblée de la République (parlement) pour un mandat de quatre ans une commission parlementaire de l'Assemblée de la République peut auditionner les directeurs du SIS et du SIEDM	l'i de da pr m
PORTUGAL	**Serviço de Informaçoes de Seguranca (SIS)** dépend du ministère de l'intérieur		service de sécurité pour les affaires intérieures; sauvegarde de la Constitution (sans compétences exécutives); collecte et analyse d'informations sur les activités criminelles et subversives			

Pays	Service de renseignement	Base juridique	Missions	Renseigne-ment électro-magnétique	Organe de contrôle	Ba
ESPAGNE	**Centro Superior de Información de la Defensa (CESID)** sous l'autorité du ministère de la défense	*R.D. 2632/1985 de 27.12.1985 (BOE 20.01.1986) Estructura interna y relaciones del Centro Superior de la Defensa;* modif. par *R.D. 266/1996 de 16.02.1996 Modif. de la estructura organica del CESID*	service de renseignement pour l'étranger et le territoire national; recherche d'informations politiques, économiques, technico-scientifiques et militaires; surveillance des services étrangers de renseignement; contre-espionnage dans le pays et à l'étranger	oui	aucun organe spécifique de contrôle; contrôle parlementaire général sous la forme de l'audition d'organes gouvernementaux par des commissions parlementaires	
ESPAGNE	**Dirección General de la Guardia Civil (GC)** sous l'autorité du ministère de la défense et du ministère de l'intérieur	*L.Org. 2/1986 de 13.03.1986 (BOE 14.03.1986) de Fuerzas y cuerpos de seguridad*	autorité centrale de police paramilitaire comportant un service de renseignement de police; lutte contre la prolifération de la criminalité organisée sur le territoire espagnol			

Pays	Service de renseignement	Base juridique	Missions	Renseigne-ment électro-magnétique	Organe de contrôle	Ba
ESPAGNE	**Dirección General de la Policia** sous l'autorité du ministère de l'intérieur		autorité centrale de police comportant un service de renseignement de police; activités de renseignement sur le territoire national et à l'étranger; lutte contre les structures terroristes et le fondamentalisme islamiste au Moyen-Orient et en Afrique du Nord			

Pays	Service de renseignement	Base juridique	Missions	Renseigne-ment électro-magnétique	Organe de contrôle
SUÈDE	**Säkerhetspolisen** (SÄPO) service civil de renseignement et de sécurité dépend du ministre de la justice	*Polislag (1984:387) Förordning (1989:773) med instruktion för Rikspolisstyrelsen* "loi (1984/387) relative aux services de police, ordonnance (1989/773) portant application de la directive relative à l'Office national de police" (NPB)	- contrôle de la sécurité - contre-espionnage - lutte contre le terrorisme - "protection de la Constitution" effectif en 1999: 800 personnes environ budget en 1995: SEK 475 millions (€ 55,7 millions)		conseil exécutif de l'Office national de police, composé de cinq parlementaires, de deux agents et du directeur général de la police nationale *Registernämnd*, composé de huit membres au maximum; siègent actuellement deux "magistrats", deux parlementaires, un avocat et un expert ces deux organes rendent compte au gouvernement
SUÈDE	**Militära Underrättelse och Säkerhetstjänsten (MUST)** "direction du renseignement et de la sécurité militaires, placée auprès de l'État major suédois Service de renseignement et de sécurité militaire sous l'autorité du ministre de la défense	Loi 2000/130 et ordonnance 2000/131 relatives aux services de renseignement militaire	Collecte et analyse d'informations militaires et politiques secrètes; contre-espionnage; lutte contre la subversion, le sabotage et les émeutes; protection des forces armées et de l'industrie de l'armement		*Försvarets underrättelsenämnd* commission de contrôle du service de renseignement de défense; composée, pour partie, de parlementaires

Pays	Service de renseignement	Base juridique	Missions	Renseigne-ment électro-magnétique	Organe de contrôle	
SUÈDE	**Försvarets Radioanstalt (FRA)** **Unité spéciale autonome (station radio)**		renseignements militaires ou autres; déchiffrement des communications; surveillance radar	oui		

Pays	Service de renseignement	Base juridique	Missions	Renseigne-ment électro-magnétique	Organe de contrôle	Ba
ROYAUME-UNI	**Government's Communication Headquarters (GCHQ)** sous l'autorité du ministre des affaires étrangères	*Intelligence Sercices Act 1994*	espionnage à l'étranger/collecte d'informations à l'étranger; renseignement électromagnétique dans les domaines politique, économique, technico-scientifique et militaire	oui	Le *Security Service Commissioner* est nommé par le premier ministre; haut juge en exercice ou honoraire. *The Investigatory Powers Tribunal*	
	Secret intelligence Service (SIS) = MI6 sous l'autorité du ministre des affaires étrangères	*Intelligence Services Act 1994*	collecte d'informations sur les activités de renseignement et les événements politiques à l'étranger		*The Intelligence and Security Committee (ISC)* La commission se compose de 9 membres (Chambre des Communes +Chambre des Lords; aucun membre ne peut être ministre), nommés par le premier ministre	

Pays	Service de renseignement	Base juridique	Missions	Renseigne-ment électro-magnétique	Organe de contrôle	Ba
ROYAUME-UNI	**Security Service = MI5** sous l'autorité du ministre de l'intérieur	*Serurity Services Acts 1989 and 1996*	collecte d'informations pour la protection de la sécurité intérieure; contre-espionnage; lutte contre les mouvements extrémistes (notamment l'IRA), le terrorisme et les éléments subversifs		*The Security Service Commissioner* *The Intelligence and Security Committee*	

Pays	Service de renseignement	Base juridique	Missions	Renseigne-ment électro-magnétique	Organe de contrôle	Ba
ROYAUME-UNI	**Defense Intelligence Staff (DIS)** sous l'autorité du ministre de la défense		soutien de la sécurité militaire; évaluation et analyse d'informations militaires, politiques et technico-scientifiques et de certaines informations économiques			

Pays	Service de renseignement	Base juridique	Missions	Renseignement électromagnétique	Organe de contrôle
ÉTATS-UNIS	**Central Intelligence Agency (CIA)**	*National Security Act 1947*	collecte de renseignements à l'échelon mondial; contre-espionnage à l'étranger; compétences centrales pour toutes les affaires relatives aux services de renseignement aux États-Unis.		*Senate*: S*enate Select Committee on Intelligence (SSCI)* *House of Representatives: House Permanent Select Committee on Intelligence (HPSCI)*
ÉTATS-UNIS	**Defense Intelligence Agency (DIA)**	créée par la *Directive 5105.21* de 1961, par le ministre de la défense *Executive Order 11905* de 1976 *DoD Directive 5105.21 1978 Executive Order 12036* *1981 Executive Order 12333*	compétente pour fournir des renseignements militaires aux troupes d'assaut et aux décideurs du ministère de la défense et du gouvernement.		S*enate Select Committee on Intelligence (SSCI)* *House Permanent Select Committee on Intelligence (HPSCI*
ÉTATS-UNIS	**National Security Agency (NSA)**	*Executive Order 12333 of 4 December 1981*	compétente pour la sécurité des systèmes d'information américains, en particulier pour le cryptage; compétente pour la surveillance des communications à l'étranger.	oui	S*enate Select Committee on Intelligence (SSCI)* *House Permanent Select Committee on Intelligence (HPSCI*
ÉTATS-UNIS	**National Imagery and Mapping Agency (NIMA)**	*National Imagery and Mapping Agency Act of 1996.*	compétente pour fournir images et cartes et les exploiter.		S*enate Select Committee on Intelligence (SSCI)* *House Permanent Select Committee on Intelligence (HPSCI*
ÉTATS-UNIS	**National Reconnaissance Office (NRO)**		compétente pour développer et mettre en œuvre des systèmes de satellites		S*enate Select Committee on Intelligence (SSCI)* *House Permanent*

Pays	Service de renseignement	Base juridique	Missions	Renseignement électromagnétique	Organe de contrôle
			d'espionnage (SIGINT, image)		*Select Committee on Intelligence (HPSCI*
ÉTATS-UNIS	**US Army Intelligence** **(p. ex. Deputy Chief of Staff for Intelligence,** **Intelligence and Security command (INSCOM)**	*Executive Order 12333* (4 décembre 1981)	collecte d'informations et analyse en matière militaire; mise au point de concepts et de systèmes de renseignement militaires et guerre électronique.	oui	*Senate Select Committee on Intelligence (SSCI)* *House Permanent Select Committee on Intelligence (HPSCI*
ÉTATS-UNIS	**Marine Corps Intelligence Activity (MCIA)** **National Maritime Intelligence Center (NMIC)**	*Executive Order 12333* (4 décembre 1981)	renseignements destinés à la Marine; renseignements militaires et mise au point de cryptage et d'auxiliaires électroniques à la guerre.	oui	*Senate Select Committee on Intelligence (SSCI)* *House Permanent Select Committee on Intelligence (HPSCI)*
ÉTATS-UNIS	**Office of Naval Intelligence (ONI)**	*Executive Order 12333* (4 décembre 1981)	renseignements à l'intention de la Navy, questions maritimes; analyse des flottes étrangères; collecte de renseignements sur les systèmes de surveillance des océans, les plates-formes sous-marines et les systèmes d'armement.	oui	*Senate Select Committee on Intelligence (SSCI)* *House Permanent Select Committee on Intelligence (HPSCI*
ÉTATS-UNIS	**Air Intelligence Agency (AIA)**	*Executive Order 12333* (4 décembre 1981)	renseignement à destination de l'Airforce; renseignement militaire	oui	*Senate Select Committee on Intelligence (SSCI)* *House Permanent Select Committee on Intelligence (HPSCI*
ÉTATS-UNIS	**Federal Bureau of Investigation (FBI)**	*Title 28, United States Code (U.S. Code)*, Section 533 créé en 1908; son nom existe depuis 1935.	contre-espionnage; police fédérale		*Senate Select Committee on Intelligence (SSCI)* *House Permanent Select Committee on Intelligence (HPSCI)*
ÉTATS-UNIS	**Drug Enforcement Administration**	*Executive Order du l^{er} juillet 1973*	collecte d'informations sur la drogue et le blanchiment d'argent sur le territoire		*Senate Select Committee on Intelligence (SSCI)* *House Permanent Select Committee on*

Pays	Service de renseignement	Base juridique	Missions	Renseignement électromagnétique	Organe de contrôle
			national et à l'étranger		*Select Committee on Intelligence (HPSCI)*
CANADA	**Communication Security Establishment (CSE);** assistée par le**Canadian Forces Supplementary Radio System (CFSRS)**	le mandat formel est classifié; il est vraisemblablement fixé avec l'accord du cabinet.	conseiller le gouvernement et les milieux économiques sur les questions de sécurité relatives à la transmission et au traitement des données (Infosec); mettre au point des systèmes de cryptage.	oui	pas d'autorité de contrôle indépendante (uniquement un contrôle par l'Auditor General et le ministre de la défense, lequel est responsable devant le parlement)
CANADA	**Canadian Security Intelligence Service (CSIS)** sous l'autorité du ministre de l'intérieur	*Canadian Security Intelligence Service Act (CSIS Act)* de 1984	contre-espionnage, lutte contre le sabotage et le terrorisme international sur le territoire national.		**The Security Intelligence Review Committee (SIRC)** organe indépendant, composé de 5 membres, qui ne sont pas des parlementaires
CANADA	**Director General Intelligence Division** (membre du *Deputy Chief of the Defence Staff)* sous l'autorité du ministre de la défense		renseignement militaire		
AUSTRALIE	**Defence Signals Directorate (DSD**) sous l'autorité du ministre de la défense		collecter et traiter les renseignements électromagnétiques; fournir au gouvernement et aux forces militaires des produits de sécurité de l'information (Infosec).		*Inspector General of Intelligence and Security (IGIS)* (nommé par le premier ministre)
AUSTRALIE	**Defence Intelligence Organisation (DIO)** sous l'autorité du ministre de la défense		collecter et évaluer informations et renseignements stratégiques et militaires		*Inspector-General of Intelligence and Security (IGIS)*
AUSTRALIE	**Australian Secret Intelligence Service (ASIS)** service d'espionnage sous l'autorité du		collecter des informations concernant l'étranger, en particulier le sud-est asiatique, dans l'intérêt de la sécurité nationale, de		*Inspector-General of Intelligence and Security (IGIS)*

Pays	Service de renseignement	Base juridique	Missions	Renseignement électromagnétique	Organe de contrôle
	ministre des affaires étrangères		l'économie et des relations extérieures.		
AUSTRALIE	**Australian Security Intelligence Organisation (ASIO)**	*The Australian Security Intelligence Organisation Act 1979 (the ASIO Act)*	protection contre la violence à motivation politique; sécurité des personnes et des biens; lutte contre le terrorisme international et le transfert illégal de technologies.		*Parliamentary Joint Committee on the Australian Security Intelligence Organization* *Inspector-General of Intelligence and Security (IGIS)*
AUSTRALIE	**Office of National Assessments** organe indépendant	*Office of National Assessments Act 1977*	fait rapport au premier ministre		*Inspector-General of Intelligence and Security (IGIS)*

Pays	Service de renseignement	Base juridique	Missions	Renseignement électromagnétique	Organe de contrôle
NOUVELLE-ZÉLANDE	**Government Communications Security Bureau (GCSB)** sous l'autorité du premier ministre	Créé en 1977. Jusqu'ici pas de base juridique; le Parlement est saisi d'une proposition (*Government Communications Security Bureau Bill*).	fourniture d'informations concernant l'étranger; sécurité des communications, sécurité informatique et de l'information (Infosec); sécurité technique.	oui	*Inspector-General of Intelligence and Security* *Intelligence and Security Committee* (premier ministre, leader de l'opposition, 3 parlementaires)
NOUVELLE-ZÉLANDE	**New Zealand Security Intelligence Service (SIS)** service de renseignement intérieur sous l'autorité du premier ministre	*New Zealand Security Intelligence Service Act 1969*	contre-espionnage; protection contre le terrorisme et la violence à motivation politique; sensibilisation des milieux scientifiques et industriels à l'espionnage industriel et au transfert illégal de technologies.		
NOUVELLE-ZÉLANDE	**External Assessments Bureau (EAB)** service de renseignement extérieur sous l'autorité du premier ministre		analyse les évolutions politiques et établit des rapports concernant les développements et tendances politiques et économiques.		
NOUVELLE-ZÉLANDE	**Directorate of Defense Intelligence and Security (DDIS)** service de renseignement		service de renseignement militaire; collecte des données importantes sur le		

Pays	Service de renseignement	Base juridique	Missions	Renseignement électromagnétique	Organe de contrôle
	militaire sous l'autorité du ministre de la défense		plan militaire, notamment dans l'espace Asie-Pacifique; analyse d'informations tactiques et stratégiques.		